UNIVERSITY OF TORONTO
3 1761 01233041 1

Verlag von B. G. Teubner in Leipzig.

Bolyai de Bolya, Ioannes, Appendix scientiam spatii absolute veram exhibens, a veritate aut falsitate axiomatis XI. Euclidei, a priori haud unquam decidenda, independentem, adiecta ad casum falsitatis quadratura circuli geometrica. Editio nova oblata ab Academia Scientiarum Hungarica ad diem natalem centesimum auctoris concelebrandum. Ediderunt Iosephus Kürschák, Mauritius Réthy, Béla Tötössy de Zebethnek, Academiae Scientiarum Hungaricae sodales. [XVI u. 154 S.] 4. 1902. geh. *M.* 4.—

[————] Libellus post saeculum quam Iohannes Bolyai de Bolya anno MDCCCII a. d. XVIII kalendas Ianuarias Claudiopoli natus est, ad celebrandam memoriam eius immortalem, ex consilio ordinis Mathematicorum et Naturae scrutatorum Regiae Litterarum Universitatis Hungaricae Francisco-Iosephinae Claudiopolitanae editus. [VIII, 40 S. u. 7 Tafeln.] 4. 1903. geh. *M.* 6.—

Wolfgangi Bolyai de Bolya Tentamen iuventutem studiosam in elementa matheseos purae elementaris ac sublimioris methodo intuitiva evidentiaque huic propria introducendi, cum appendice triplici. Editio secunda. Tomus I: Conspectus arithmeticae generalis. Mandato academiae scientiarum hungaricae suis adnotationibus adiectis ediderunt Iulius König et Mauritius Réthy, academiae scientiarum hungaricae sodales. Mit dem Bildnis des Verfassers und 11 lithograph. Tafeln. [XII u. 679 S.] 4. 1897. In Halbkalbleder geb. n. *M.* 40.—

Briefwechsel zwischen Carl Friedrich Gauſs und Wolfgang Bolyai. Mit Unterstützung der Königl. Ungarischen Akademie der Wissenschaften herausgegeben von Franz Schmidt und Paul Stäckel. [XVI u. 208 S.] 4. 1899. In Halbkalblederband geb. n. *M.* 16.—

Mathematische und naturwissenschaftliche Berichte aus Ungarn. Mit Unterstützung der Ungarischen Akademie der Wissenschaften und der Kgl. Ungarischen Naturwissenschaftlichen Gesellschaft. Gegenwärtig redigiert von Prof. Aug. Heller in Budapest. gr. 8. geh.

1. Bd.	1882/83.	[419 S. m. H. u. L.]	*M.* 10.—	10. —	1891/92.	[419 S. m. 7 Taf.]	*M.* 8.—
2. —	1883/84.	[482 S. m. 10 L.]	„ 8.—	11. —	1892/93.	[491 S. m. 25 Taf.]	„ 8.—
3. —	1884/85.	[320 S.]	„ 6.—	12. —	1893/94.	[XVI u. 478 S. m. Abb.]	„ 8.—
4. —	1885/86.	[303 S. m. 3 Taf.]	„ 6.—	13. —	1894/95.	[IV u. 464 S. m. Abb.]	„ 8.—
5. —	1886/87.	[323 S. m. 5 Taf.]	„ 6.—	14. —	1895/96.	[XVI u. 437 S. m. Fig.]	„ 8.—
6. —	1887/89.	[509 S. m. 4 Taf.]	„ 8.—	15. —	1897.	[XI u. 459 S. m. Fig. u. 3 Taf.]	„ 8.—
7. —	1888/89.	[525 S. m. 4 Taf.]	„ 8.—	16. —	1898.	[X u. 372 S.]	„ 7.—
8. —	1889/90.	[525 S. m. 9 Taf.]	„ 8.—	17. —	1899.	[VII u. 364 S.]	„ 8.—
9. —	1890/91.	[478 S. m. 8 Taf.]	„ 8.—	18. —	1900.	[X u. 477 S.]	ca. „ 8.—

☞ Im Verlage von B. G. Teubner in Leipzig ist erschienen und durch jede Buchhandlung zu beziehen:

Niels Henrik Abel,

Oeuvres complètes. Nouvelle édition publiée aux frais de l'État Norvégien par MM. L. Sylow et S. Lie. 2 tomes. 4. 1881. geh. *M.* 24.—

Tome premier [VIII u. 621 S.], contenant les mémoires publiés par Abel.
Tome second [IV u. 341 S.], contenant les mémoires posthumes d'Abel.

Carl Friedrich Gauss,

Werke. Herausgegeben von der Kgl. Gesellschaft der Wissenschaften zu Göttingen. 10 Bände. gr. 4. kart.

Bisher erschienen:

Band I: Disquisitiones arithmeticae. 2. Abdr. 1876. *M.* 20.—
„ II: Höhere Arithmetik. 2. Abdruck 1876. *M.* 20.—
„ III: Analysis. 2. Abdruck 1876. *M.* 20.—
„ IV: Wahrscheinlichkeits-Rechnung und Geometrie. 1873. *M.* 25.—
Band V: Mathemat. Physik. 2. Abdruck 1877. *M.* 25.—
„ VI: Astron. Abhandlungen. 1874. *M.* 33.—
„ VIII: Nachträge zur Arithmetik, Analysis, Wahrscheinlichkeitsrechnung und Geometrie. 1900. *M.* 24.—

Nachtrag zum ersten Abdruck des zweiten Bandes 1876 kart. *M.* 2.—
Band VII, IX u. X folgen in den nächsten Jahren.

Hermann Grassmann,

gesammelte mathematische und physikalische Werke. Auf Veranlassung der Kgl. Sächsischen Gesellschaft der Wissenschaften herausg. von Friedrich Engel. In 3 Bänden. I. Band. In 2 Theilen. gr. 8. geh. *M.* 28.—

I. Band. I. Theil: Die Ausdehnungslehre von 1844 und die geometrische Analyse. Mit einem Bilde Grassmanns in Holzschnitt u. 35 Figuren im Text. [XV u. 435 S.] 1894. *M.* 12.—
I. — II. — Die Ausdehnungslehre von 1862. Mit 37 Figuren im Text. [VIII u. 511 S.] 1896. *M.* 16.—
[Fortsetzung unter der Presse.]

Leopold Kronecker,

Werke. Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von Kurt Hensel. In 4 Bänden. 4. geh.

I. Band, mit dem Bildnisse Kroneckers. [IX u. 484 S.] 1895. *M.* 28.—
II. — [VIII u. 541 S.] 1897. *M.* 36.—
III. — 1. Halbband. [VIII u. 473 S.] 1899. *M.* 36.—
[Fortsetzung unter der Presse.]

Julius Plücker,

gesammelte wissenschaftliche Abhandlungen. Im Auftrag der Kgl. Gesellschaft der Wissenschaften zu Göttingen herausgegeben von A. Schoenflies und Fr. Pockels. In 2 Bänden. gr. 8. geh. *M.* 50.—

I. Band. Mathematische Abhandlungen, herausgegeben von A. Schoenflies. Mit einem Bildnisse Plückers u. 73 in d. Text gedruckten Fig. [XXXV u. 620 S.] 1895. *M.* 20.—
II. — Physikalische Abhandlungen, herausgegeben von Fr. Pockels. Mit 78 in den Text gedruckten Figuren und 9 lithogr. Tafeln. [XVIII u. 834 S.] 1896. *M.* 30.—

Bernhard Riemann,

gesammelte mathematische Werke und wissenschaftlicher Nachlass. Herausgegeben von Heinrich Weber. Zweite Auflage bearbeitet von Heinrich Weber. Mit einem Bildniss Riemanns. [X u. 558 S.] gr. 8. 1892. geh. *M.* 18.—

EINLEITUNG
IN DIE ALLGEMEINE THEORIE DER
ALGEBRAISCHEN GRÖSZEN

VON

JULIUS KÖNIG

AUS DEM UNGARISCHEN ÜBERTRAGEN VOM VERFASSER

12870
2|7|12

LEIPZIG
DRUCK UND VERLAG VON B. G. TEUBNER
1903

QA
201
K615

ALLE RECHTE,
EINSCHLIESZLICH DES ÜBERSETZUNGSRECHTS, VORBEHALTEN.

Vorrede.

Die allgemeine Theorie der algebraischen Größen hat Leopold Kronecker in der berühmten „Festschrift“ vom Jahre 1882 nicht nur als grundlegende mathematische Disziplin neu geschaffen, sondern auch ihrem gesamten Inhalte, ihren Zielen und Problemen nach genau umschrieben. Gleichwohl reicht die Geschichte ihrer Entwicklung weit zurück. Als verschleiertes Bild in Gauß' unvergänglichen Arbeiten enthalten, hat diese Theorie in den arithmetischen Untersuchungen von Lejeune-Dirichlet, Kummer und Dedekind, den algebraischen Forschungen von Abel, Galois und Jordan, den funktionentheoretischen Schöpfungen von Puiseux, Riemann und Weierstraß, sowie endlich in den algebraisch-geometrischen Sätzen von Cayley, Clebsch, Gordan und Noether ihre entscheidenden Gesichtspunkte gewonnen. Auch die seit dem Erscheinen der Festschrift verflossenen weiteren zwei Jahrzehnte haben bedeutsame Resultate geliefert, aus denen — abgesehen von den Kroneckerschen Abhandlungen — insbesondere die geradezu grundlegenden Sätze über Divisorensysteme von Hilbert und die wertvollen Arbeiten von Hensel hervorzuheben sind.

Bedenkt man weiter, daß auch die neuen Bahnen, welche die Gruppen- und Funktionentheorie unter der Führung von Klein und Lie einerseits, Fuchs und Poincaré andrerseits eingeschlagen hat, mit der Theorie der algebraischen Größen vielfache Berührungs- und Kreuzungspunkte aufweist, so ergibt sich für unsre Disziplin eine zentrale Stellung, die an Bedeutung auf dem Gebiete der reinen Mathematik vielleicht nur von den Methoden der Infinitesimalrechnung übertroffen wird.

Eine systematische Darstellung der Theorie — oder genauer ausgedrückt ihrer Fundamentalsätze —, die sich in allerdings unvollkommener Analogie zu den gangbaren arithmetisch-algebraischen Handbüchern so verhält, wie eine Darstellung der Funktionentheorie zu den Lehrbüchern der Differential- und Integralrechnung, wird wohl ohne weiteres als dankbare Aufgabe anerkannt werden. Wie schwierig eine befriedigende Lösung dieser Aufgabe sich gestaltet, hat der Verfasser des

vorliegenden Versuchs an seiner Arbeit selbst erfahren. War ja doch neben manchen methodischen Fragen früher eine Reihe von Fundamentalproblemen zu erledigen, deren Lösung entweder gar nicht, oder nur für spezielle Fälle bekannt war.

Gerade diese neuen Untersuchungen, die wohl mehr als die Hälfte des gesamten Inhaltes ausmachen, drängten aber zu der hier gewählten systematischen Darstellung. Seit langer Zeit mit dem Gegenstande beschäftigt, mußte ich bald einsehen, daß einzelne Abhandlungen bei dem vielfachen Ineinandergreifen jener Fundamentalprobleme wieder sehr schwer lesbar und auf einen kleinsten Kreis beschränkt blieben, also ihren Hauptzweck verfehlen müßten. Denn als solchen betrachte ich es, den Geist der Kroneckerschen Methoden — wenn der Ausdruck für dieses schwierige mathematische Gebiet gestattet ist — zu popularisieren.

So entstand dieses Buch, das eigentlich nur die ersten Elemente der Algebra und Zahlentheorie — einige Sätze aus der Lehre von den Determinanten inbegriffen — voraussetzt, und das eben darum auch ein Studierender mit Nutzen lesen kann; während andrerseits der Fachmann die Darstellung alter und neuer Resultate hier in bequemerer Form erhält, als dies in einzelnen Journalabhandlungen hätte geschehen können.

Den Inhalt des Buches hier in Form eines noch so knappen Referates zusammenzufassen, hieße den Umfang dieser Vorrede zu sehr ausdehnen; statt dessen sollen hier nur einige Punkte fragmentarisch berührt werden.

Die ganze Darstellung geht von der Definition „holoider“ und „orthoider“ Bereiche aus, die den Bereichen der ganzen rationalen, resp. der rationalen Zahlen nachgebildet sind, also, wie es scheint, durch gangbare technische Ausdrücke wie Integritätsbereich und Rationalitätsbereich (Körper) ersetzt werden können. Daß dies nicht der Fall ist, wird der aufmerksame Leser bald erkennen; denn jene Definitionen vermeiden die Starrheit der letzteren Begriffe und gestatten infolgedessen eine viel einfachere Grundlegung der Theorie, heben den unangenehmen Gegensatz zwischen Arithmetik und Geometrie und ergeben den für die Ökonomie der Darstellung wichtigen Umstand, daß das „Orthoide“ (Rationale) als spezieller Fall des „Holoiden“ (Ganzen) zu betrachten ist. Diesen Begriffsbestimmungen entsprechend scheidet sich auch die Theorie in einen „algebraischen“ und „arithmetischen“ Teil.

Vom methodischen Standpunkte aus möchte ich noch hervorheben, daß der Kroneckersche Fundamentalsatz

(Kap. III. § 5—7) auf Grund eines völlig elementaren Beweises zum Ausgangspunkt der ganzen Theorie gewählt werden konnte.

Diesem Satze reiht sich sodann — als wichtigste Grundlage der hier erlangten neuen Resultate — die Aufstellung der von mir sogenannten Resolventenform an, die als für ein beliebiges Formensystem geltende arithmetische Erweiterung des Resultantenbegriffs aufzufassen ist und insbesondere immer als homogene lineare Form der gegebenen Formen dargestellt werden kann. Dabei wird nach dem Beispiele Kroneckers bei Benutzung des Ausdrucks „Form" von der Forderung der Homogeneität abgesehen.

Die Einführung der Resolventenform einerseits, der Kroneckersche Grundgedanke der Association neuer Unbestimmter andrerseits führen zu einer — im vollen Sinne des Wortes — allgemeinen Theorie der Elimination, in der die Multiplizität der durch irgend ein Gleichungssystem definierten Mannigfaltigkeiten nicht mehr, wie dies in der „Festschrift" der Fall ist, vernachlässigt wird. So entsteht ein mächtiges Werkzeug der Forschung, das uns zunächst eine rein algebraische Theorie der Funktionaldeterminanten liefert. In einem längeren Exkurse wird dann auch eine definitive Darstellung der sog. speziellen Eliminationstheorie, d. h. die allgemeine Theorie der Resultanten und Discriminanten — letztere zum ersten Male — gegeben.

Die im engeren Sinne des Wortes arithmetischen Teile der Theorie erhalten durch die Behandlung der linearen diophantischen Probleme eine feste Grundlage. Als solches wird die allgemeine Lösung eines Gleichungssystems hingestellt, dessen einzelne Gleichungen die Gestalt $\Sigma F_i X_i = F$ haben. Dabei sind die F als gegebene, die X als unbekannte Formen angesehen, die der weiteren Bedingung unterworfen sind, daß ihre Koeffizienten einem bestimmten, vorweg gegebenen holoiden Bereiche angehören. Dieses Problem wird in den für die Theorie der algebraischen Größen ausreichenden Fällen durch eine endliche, wohldefinierte Reihe elementarer Operationen vollständig gelöst. Es sind dies die Fälle, wo die Formenkoeffizienten entweder einem orthoiden Bereiche (also z. B. irgend einem Rationalitätsbereiche) oder aber dem Bereiche der ganzen rationalen Zahlen angehören.

Der erste Fall ergibt unter anderem eine allgemeine Behandlung des Noetherschen Satzes im Raume von n Dimensionen.

Mit diesen Resultaten ist nicht nur die wichtige, bisher kaum gestreifte Frage nach der Äquivalenz zweier Divisorensysteme vollständig gelöst, sondern es ist auch die allgemeinere

Frage des „Enthaltenseins“ eines Divisorensystems in einem andern erledigt.

In der Theorie der ganzen algebraischen Größen werden die beiden Fälle der im strengen Sinne der allgemeinen Arithmetik („absolut“) ganzen Größen und der in Bezug auf einen orthoiden Bereich („relativ“) ganzen Größen zugleich und nach denselben Methoden behandelt. Im zweiten Falle sind unter anderen die im Sinne der Funktionentheorie oder Geometrie ganzen Größen enthalten. Es ist ein Kardinalpunkt der Darstellung, daß die idealen Größen von Beginn ab als nicht nur der Multiplikation, sondern auch der Addition fähige Größen eingeführt werden. Auf dieser Grundlage baut sich eine wesentlich neue und einfache Methode zur wirklichen Bestimmung des Fundamentalsystems in allen Fällen auf, die in erster Reihe auf der Theorie des „Äquivalenzmoduls“ beruht. Die Zerlegung einer ganzen Größe in Primideale wird endlich definitiv und ohne Ausnahmefall geleistet, wobei die diesbezüglichen Kroneckerschen Resultate in einem wesentlichen Punkte richtig zu stellen sind, da diese infolge eines merkwürdigen, allerdings tiefer liegenden Versehens nur in den einfachsten Fällen richtig sind.

Für alles Weitere sei auf das Inhaltsverzeichnis verwiesen, aus dem der Inhalt des Buchs und dessen Disposition im einzelnen zu ersehen ist. Ein ausführliches Sachregister wird — wie ich hoffe — die Benutzung des Buches wesentlich erleichtern und insbesondere in Bezug auf die Terminologie, in der einige Neuerungen leider unvermeidlich waren, bequeme Verweisungen bieten.

Literaturnachweise konnten — mit Rücksicht auf die im Erscheinen begriffene „Encyklopädie“ — auf das Notwendigste beschränkt werden und sind nur soweit geführt, als es die Klarstellung des Besitzstandes bei jedem einzelnen Satze erforderte.

Es bleibt mir nur noch übrig, den Herren J. Kürschák, G. Rados, I. Rados und P. Stäckel für ihre unermüdliche und äußerst wertvolle Beihilfe bei der Revision des Manuskripts und der Korrekturen, sowie der B. G. Teubnerschen Verlagsbuchhandlung für ihr auch hier bewährtes liebenswürdiges Entgegenkommen meinen besten Dank abzustatten und endlich zu bemerken, daß das ursprüngliche, in ungarischer Sprache abgefaßte Werk zugleich von der Ungarischen Akademie der Wissenschaften veröffentlicht wird.

Budapest, Juni 1902. **Julius König.**

Inhaltsverzeichnis.

Erstes Kapitel.

Einleitende Grundbegriffe.

		Seite
§ 1.	Zahl, Größe, Bereich	1
§ 2. 3.	Das gewöhnliche Additions- und Multiplikationsgesetz	4 5
§ 4.	Holoide und orthoide Bereiche	7
§ 5.	Teilbarkeit in holoiden Bereichen	9
§ 6.	Der größte gemeinschaftliche Teiler	13
§ 7—9.	Beispiel: Die Bereiche $[\sqrt{-k}]$	15 19 21
§ 10. 11.	Kongruenzbereiche und Modulsysteme	23 26
§ 12.	Relative Äquivalenz	27

Zweites Kapitel.

Holoiden Bereichen entstammende Formen.

§ 1. 2.	Formen und ganze Funktionen	31 33
§ 3. 4.	Lexikographische Anordnung der Glieder einer Form.	35 37
§ 5. 6.	Die derivierten Formen	38 40
§ 7.	Der polynomische Lehrsatz	42
§ 8. 9.	Homogene Formen	43 45
§ 10—12.	Die elementaren symmetrischen Formen	46 47 50
§ 13—16.	Die reduzierten Formen	54 56 58 60
§ 17.	Die ganzen Funktionen	62
§ 18. 19.	Lineare Transformation. Reguläre Formen	65 67

Drittes Kapitel.

Die Teilbarkeit der Formen.

§ 1.	Das gewöhnliche Divisionsverfahren	70
§ 2. 3.	Das Kriterium der Teilbarkeit im Formenbereiche	72 73
§ 4.	Der Dedekindsche Hilfssatz	74
§ 5—7.	Der Kroneckersche Fundamentalsatz	78 80 82

Seite

§ 8—11. Vollständigen Bereichen entstammende Formen 83 86 88 89
§ 12. Vollständigen Bereichen zugeordnete orthoide Bereiche . 91
§ 13—17. Die Resultante 93 95 98 100 101
§ 18. Die Resolventenform eines Formensystems 102
§ 19—21. Das Problem der Theorie der Gleichungen . . 108 110 115
§ 22. 23. Die Discriminante einer Form 117 119
§ 24. 25. Resultante und Discriminante als symmetrische Form 122 125

Viertes Kapitel.

Die algebraischen Größen.

§ 1. 2. Faktorenzerlegung der rationalen und ganzen Formen 127 129
§ 3. 4. Faktorenzerlegung in orthoiden Formenbereichen . . 131 134
§ 5 — 7. Neue Fassung des Gleichungsproblems. Adjunktion 136 138 141
§ 8. 9. Hyperorthoide Bereiche 144 148
§ 10—13. Der Galoissche Bereich 149 154 157 158
§ 14. 15. Die Gattungsbereiche 159 162
§ 16—19. Gattungsbereiche, deren Stammbereich selbst schon ein Gattungsbereich ist 164 167 170 172
§ 20—22. Die Rationalitätsbereiche 174 178 180
§ 23—26. Das Galoissche Prinzip 184 188 190 192
§ 27. 28. Der Gaußsche Fundamentalsatz 194 197

Fünftes Kapitel.

Allgemeine Theorie der Elimination.

§ 1. Das fundamentale Problem. 199
§ 2 — 4. Die Kroneckersche Eliminationsmethode . . . 201 205 207
§ 5 — 8. Die Gesamtheit der Lösungen des Systems $F_j = 0$ 212 215 220 224
§ 9. 10. Die Hauptdarstellungen reiner Mannigfaltigkeiten . . 228 232
§ 11. Die vollständige Darstellung beliebiger Mannigfaltigkeiten durch $m + 1$ Gleichungen 234
§ 12. 13. Gleichungssysteme, deren Inhalt eine lineare Mannigfaltigkeit bildet 238 240
§ 14—18. Die Funktionaldeterminante 243 247 252 255 257

Sechstes Kapitel.

Resultanten und Discriminanten.

(Spezielle Eliminationstheorie.)

§ 1. 2. Allgemeine Formen und die diesbezügliche Fragestellung 260 263

Seite

§ 3—6. Definition und fundamentale Eigenschaften der Resultante 265 268 270 274
§ 7—10. Rekursive Bildung der Resultante 275 280 282 285
§ 11. Der Produktsatz der Resultantentheorie 288
§ 12. Resultante eines Systems homogener Formen. Invarianteneigenschaft 291
§ 13. Systeme homogener Gleichungen 294
§ 14—17. Bestimmte und unbestimmte gewöhnliche Systeme 299 302 308 310
§ 18—21. Symmetrische Formen von mehreren Größensystemen 312 315 317 321
§ 22. Die Irreduzibilität der Funktionaldeterminante 323
§ 23—26. Die Grundeigenschaften der Discriminante . 325 326 329 330
§ 27. Die Invarianteneigenschaft der Discriminante 335
§ 28—30. Die Multiplizität der Lösungen 338 341 342

Siebentes Kapitel.

Lineare diophantische Probleme.

(Allgemeine Sätze und die algebraische Theorie.)

§ 1. Aufstellung des Problems 347
§ 2—4. Modul- oder Divisorensysteme 351 354 358
§ 5—7. Endliche Divisorenketten 362 367 368
§ 8. Sonderung der algebraischen und arithmetischen Probleme 371
§ 9. Algebraische Theorie der linearen diophantischen Systeme 373
§ 10. 11. Die Divisorensysteme der Hauptklasse (deren Elemente einem orthoiden Bereiche entstammende Formen sind) 377 381
§ 12. 13. Der verallgemeinerte Noethersche Satz 385 389
§ 14. 15. Theorie der Charakteristiken der Wurzelsysteme für den „einfachen“ Fall 393 394
§ 16. Der Hilbertsche Satz 398

Achtes Kapitel.

Arithmetische Theorie der linearen diophantischen Probleme.

§ 1—4. Die absoluten Primsysteme in $[(1), x_1, x_2, \ldots, x_k]$ 401 404 409 413
§ 5. Divisorensysteme mod. $(P^{(k)})$ 416
§ 6—8. Theorie der Resolventenformen mod. $(P^{(k)})$ . . 419 422 428
§ 9. Gattungsbereiche mod. $(P^{(k)})$ 431
§ 10—14. Arithmetische Theorie der homogenen linearen diophantischen Gleichungen. Die Prinzipien der Reduktion 435 438 441 442 444

Seite

§ 15—18. Der allgemeine Fall 447 449 451 454
§ 19. Der singuläre Fall 456

Neuntes Kapitel.

Die ganzen algebraischen Größen.

§ 1. Einleitende Festsetzungen 459
§ 2. 3. Die ganzen algebraischen Größen und Formen . . 463 466
§ 4 — 6. Die primitiven ganzen algebraischen Formen . 468 470 473
§ 7 — 9. Die Association der idealen Größen 474 479 482
§ 10—13. Teilbarkeitstheorie der Ideale 484 487 489 491
§ 14—16. Das Fundamentalsystem der wirklichen Größen eines Gattungsbereichs 493 497 501
§ 17—20. Teilbarkeit der Formen nach einem Äquivalenzmodul 502 505 506 510
§ 21—23. Allgemeine Methode zur Aufstellung der Fundamentalsysteme 512 518 520
§ 24. 25. Das Fundamentalsystem der idealen Größen eines Gattungsbereichs 524 530
§ 26—29. Die Zerlegung der ganzen Größen in Primideale 534 539 542 545
§ 30. 31. Die Discriminante der Gattung 547 550

Namen- und Sachregister 553

Erstes Kapitel.

Einleitende Grundbegriffe.

Zahl, Größe, Bereich.

§ 1. Der Bereich der rationalen Zahlen, d. h. der Inbegriff der positiven oder negativen, ganzen oder gebrochenen Zahlen, mit Einschluß der Null, bildet die Grundlage aller Forschung auf dem Gebiete der reinen Mathematik.

Die Gesamtheit der Gesetze, nach denen die Verknüpfung dieser Zahlen in den vier Species geschieht, — und nur diese mit ihren Folgesätzen — bildet den Inbegriff der Eigenschaften, die wir dem Bereiche der rationalen Zahlen zuschreiben.

Zahl im allgemeinsten Sinne des Wortes heißt jeder Begriff, dessen Inhalt durch eine Reihe von rationalen Zahlen — oder also auch in letzter Analyse durch eine Reihe von positiven ganzen Zahlen — vollständig beschrieben werden kann; die Zahl heißt — im allgemeinsten Sinne des Wortes — algebraisch, wenn diese vollständige Beschreibung mit Hilfe einer endlichen Anzahl ganzer Zahlen geschehen kann.

Diese Definition der algebraischen Zahl und weiter unten der algebraischen Größe kann der Natur der Sache nach nur provisorisch und lückenhaft sein; denn es wird ja die Aufgabe des ganzen vorliegenden Buches sein, den Begriff der algebraischen Größe aufzubauen und seinen Inhalt zu entwickeln. Sie ist jedenfalls viel zu weit; denn wenn auch jene vollständige Beschreibung mit Hilfe einer endlichen Anzahl ganzer Zahlen jedenfalls so zu verstehen ist, daß als Eigenschaften der letzteren nur ihre Verknüpfungen in den vier Species zu

verstehen sind, so ist damit noch keineswegs festgestellt, welcher Art jene Eigenschaften des neuen Begriffs sind, die in dessen vollständige Beschreibung eingehen. Es werden als solche gewisse, den vier Species analoge Verknüpfungen festzusetzen sein, was aber schon ausführlichere Erläuterungen erheischt.

Als (mathematische) Größe bezeichnen wir eine Zahl, wenn einige ihrer Bestimmungsstücke, die natürlich selbst Zahlen sind, unbestimmt bleiben. Im einfachsten Fall heißt also eine unbestimmte ganze oder rationale Zahl selbst Größe. (Größen sind ferner — wenn wir der in Aussicht genommenen Begriffsbildung vorgreifen — z. B. alle ganzen Funktionen der Unbestimmten $x_1, \ldots, x_m$ mit bestimmten Zahlenkoeffizienten). Der kürzeren Ausdrucksweise wegen soll endlich in den Begriff der „Größe" auch die „Zahl" eingeschlossen sein.

Eine algebraische Größe ist demnach inhaltlich durch eine endliche Reihe von bestimmten und unbestimmten ganzen Zahlen festgelegt.*)

Als allgemeinster Gegenstand arithmetisch-algebraischer Forschung kann dann die Theorie derjenigen ganzen Funktionen bezeichnet werden, deren Koeffizienten selbst wieder algebraische Größen sind.

Wir wollen jedoch die in Aussicht genommenen Begriffsbildungen einer weiteren Beschränkung unterwerfen.

Der Bereich, in dem sich jede einzelne unserer Untersuchungen bewegt, d. h. die Gesamtheit aller Größen, die wir zu gleicher Zeit überblicken, soll ein solcher sein, daß in ihm gewisse charakteristische Eigenschaften des Bereiches der rationalen

*) In diesem Sinne sollen hier — nach Kronecker — die Bezeichnungen Größe und algebraische Größe benutzt werden. Außerhalb des Gebietes der Arithmetik und Algebra werden diese Ausdrücke in weiterem Sinne benutzt. So heißt Größe jede Eigenschaft der Dinge, die durch Zahlen vollständig beschrieben werden kann. In der Funktionentheorie bezeichnet man als algebraische Funktionen auch solche Größen, die durch eine endliche Anzahl bestimmter und unbestimmter Zahlen definiert sind, ohne daß diese algebraisch sein müßten.

Zahlen erhalten bleiben. Genauer ausgedrückt: Für die Größen des betrachteten Bereichs sollen nur solche Verknüpfungen festgesetzt werden, deren formale Gesetze mit denen der vier Species im Bereiche der rationalen Zahlen vollständig übereinstimmen.

Es ist dann am bequemsten, jene Verknüpfungen, soweit sie überhaupt vorhanden sind, auch in dem neuen Bereiche als Addition, Subtraktion, Multiplikation oder Division zu bezeichnen.

Am Ausgangspunkt unsrer Untersuchungen kennen wir nur den Bereich der ganzen Zahlen und den Bereich der rationalen Zahlen, deren Inhalt und Eigenschaften die Elemente ergeben; und in strenger methodischer Observanz dürfen wir erst dann von den Verknüpfungen der Größen eines neuen Bereichs sprechen, wenn diese Größen in jedem einzelnen Falle vollständig definiert sind, was übrigens, da jene Verknüpfungen die einzigen in Betracht kommenden „Eigenschaften" jener Größen sind, eben nur durch Feststellung jener Verknüpfungsgesetze geschehen kann. Mit einem Worte, jede weitere Entwicklung müßte an bestimmten, speciellen neuen Begriffsbildungen geschehen. Um aber die hiermit verbundenen weitläufigen Wiederholungen zu vermeiden, sollen jene großen Klassen von Bereichen, mit denen wir es immer wieder zu thun haben, ein für allemal charakterisiert und mit Namen belegt werden; doch soll dies jetzt nur für die einfachsten Fälle geschehen; die Erörterung komplizierter Verhältnisse, die ohne eigentliches Substrat keine rechte Einsicht gewährt, bleibt vorbehalten.

Dabei sei noch erwähnt, daß diese eigentlich noch der mathematischen Logik angehörenden Festsetzungen weit über den Rahmen der Arithmetik und Algebra hinausgreifen, und demnach eine große Reihe unsrer späteren Untersuchungen auch auf dem weiteren Gebiete der Analysis ihre Geltung bewahrt.

Das gewöhnliche Additions- und Multiplikationsgesetz.

§ 2. Es sei demnach eine (begrenzte oder unbegrenzte) Reihe von Größen

$$\alpha_1, \quad \alpha_2, \quad \alpha_3, \quad \ldots$$

gegeben*), deren Gesamtheit den Bereich A bildet.

Der Bereich A besitzt ein gewöhnliches Additionsgesetz, wenn die folgenden Bedingungen erfüllt sind:

a) Einer gegebenen Festsetzung gemäß bestimmen zwei Größen des Bereichs, α_1 und α_2, immer eine dritte Größe des Bereichs, σ, die die Summe von α_1 und α_2 genannt wird und mit $\alpha_1 + \alpha_2$ bezeichnet werden soll.

b) Es ist

$$\alpha_1 + \alpha_2 = \alpha_2 + \alpha_1$$

und

$$(\alpha_1 + \alpha_2) + \alpha_3 = \alpha_1 + (\alpha_2 + \alpha_3);$$

in bekannter Ausdrucksweise: Das Additionsgesetz ist kommutativ und associativ.

c) Sind α_1 und α_2 zwei beliebige Größen des Bereichs, so gibt es eine und nur eine Größe ξ von der Beschaffenheit, daß

$$\alpha_1 + \xi = \alpha_2$$

wird; in bekannter Ausdrucksweise: Die Umkehrung der Addition, die Subtraktion, ist eindeutig und immer ausführbar. Wir schreiben dann

$$\xi = \alpha_2 - \alpha_1.$$

Die Summe $\alpha_1 + \alpha_2 + \cdots + \alpha_n$, die zuerst rekursiv als $(\alpha_1 + \cdots + \alpha_{n-1}) + \alpha_n$ zu definieren ist, erweist sich nach einer Schlußweise, die wohl zuerst von Lejeune-Dirichlet genau formuliert wurde**), als von der Reihenfolge der Summanden $\alpha_1, \ldots, \alpha_n$ unabhängig.

---

*) Die Benutzung der Indices soll durchaus nicht an eine festgelegte Reihenfolge der Elemente oder gar an eine eindeutige Beziehung auf die Reihe der ganzen Zahlen („Abzählbarkeit") erinnern; sie geschieht lediglich aus Bequemlichkeitsgründen.

**) Vorlesungen über Zahlentheorie von P. G. Lejeune-Dirichlet, herausgegeben von R. Dedekind, IV. Aufl. pag. 3.

Wenn α eine beliebige Größe ist und 0 eine solche Größe bezeichnet, daß immer

$$\alpha + 0 = \alpha$$

ist, so folgt aus den angegebenen Bedingungen die Existenz einer und nur einer solchen „Null" genannten Größe. Diese wird, wenn α_1 eine bestimmte Größe ist, jedenfalls durch die Bedingung

$$\alpha_1 + 0 = \alpha_1$$

eindeutig bestimmt; ist α_2 nun irgend eine zweite Größe, so ist die Größe β wieder durch die Bedingung

$$\alpha_1 + \beta = \alpha_2$$

festgelegt, und man hat

$$\alpha_1 + 0 + \beta = \alpha_1 + \beta$$

oder endlich:

$$\alpha_2 + 0 = \alpha_2 .$$

§ 3. Der Bereich A besitzt ein gewöhnliches Multiplikationsgesetz, wenn die folgenden Bedingungen erfüllt sind:

a) Einer gegebenen Festsetzung gemäß bestimmen zwei Größen des Bereichs immer eine dritte Größe des Bereichs, π, welche das Produkt von α_1 und α_2 genannt wird und mit $\alpha_1 \alpha_2$ bezeichnet werden soll.

b) Es ist

$$\alpha_1 \alpha_2 = \alpha_2 \alpha_1$$

und

$$(\alpha_1 \alpha_2) \alpha_3 = \alpha_1 (\alpha_2 \alpha_3) ;$$

in bekannter Ausdrucksweise: Das Multiplikationsgesetz ist kommutativ und associativ.

c) Wenn der Bereich A zugleich ein gewöhnliches Additionsgesetz besitzt, so ist

$$(\alpha_1 + \alpha_2)\, \alpha_3 = \alpha_1 \alpha_3 + \alpha_2 \alpha_3 ;$$

in bekannter Ausdrucksweise: Das Multiplikationsgesetz ist in diesem Falle auch distributiv.

d) Es gibt keine, oder nur eine singuläre Größe δ, für die $\delta\xi = \delta\eta$ ist, obwohl die bestimmten Größen ξ und η verschieden sind.

Ist α eine beliebige Größe, so folgt aus $\delta\xi = \delta\eta$ auch

$$(\delta\alpha)\xi = (\delta\alpha)\eta\,.$$

Unsern Festsetzungen gemäß muß also für ein beliebiges α auch

$$\delta\alpha = \delta$$

sein. Die singuläre Größe δ kann demnach als 0 bezeichnet werden. Dieses Zeichen ist nur für den Fall schon benutzt, wenn der Bereich auch ein gewöhnliches Additionsgesetz besitzt. Dann ist aber

$$(\beta + 0)\alpha = \beta\alpha + 0\,.\,\alpha = \beta\alpha;$$

also $0\,.\,\alpha = 0$; und, da nicht mehr als eine singuläre Größe existiert, $\delta = 0$.

In Bereichen mit gewöhnlichem Multiplikationsgesetz kann demnach nur dann $\alpha\beta = 0$ sein, wenn $\alpha = 0$ oder $\beta = 0$; denn aus $\alpha\beta = 0$ und $\alpha\,.\,0 = 0$ folgt, wenn α nicht Null ist, $\beta = 0$.

Es sei noch erwähnt, daß jedes „Produkt“ $\alpha_1\alpha_2 \ldots \alpha_n$, das zuerst rekursiv durch $(\alpha_1 \ldots \alpha_{n-1})\,\alpha_n$ zu definieren ist, nach der schon bei der Addition citierten Schlußweise sich als von der Reihenfolge der Faktoren $\alpha_1, \alpha_2, \ldots \alpha_n$ unabhängig erweist.

Sind ε und ξ zwei bestimmte, von 0 verschiedene Größen des Bereichs A, deren Produkt $\varepsilon\xi = \xi$ ist, so muß, wenn α eine beliebige Größe ist, auch $\varepsilon\alpha = \alpha$ sein, denn aus

$$\varepsilon\xi = \xi, \qquad \varepsilon\alpha = \beta,$$

wo β von α verschieden ist, würde

$$(\varepsilon\xi)\beta = (\varepsilon\xi)\alpha$$

folgen, und hieraus im Widerspruch zur Annahme $\varepsilon\xi = 0$. Keinesfalls existiert eine zweite Größe ε_1 mit ähnlichen Eigenschaften; denn es ist dann $\varepsilon\varepsilon_1 = \varepsilon = \varepsilon_1$.

Die Größe ε soll, wenn sie überhaupt in A vorkommt, die absolute Einheit des Bereichs heißen und mit 1 bezeichnet werden.

Holoide und orthoide Bereiche.

§ 4. Ein Bereich heiße holoid*), wenn er ein gewöhnliches Additions- und Multiplikationsgesetz besitzt, die absolute Einheit enthält und die durch wiederholte Addition der 1 entstehende Größenreihe

$$1,\ 1+1,\ 1+1+1,\ 1+1+1+1,\ \cdots$$

die Größe 0 nicht enthält.

Wir können — zuerst vorläufig — zur Bezeichnung dieser Größen die Zeichen der gewöhnlichen ganzen Zahlen

$$(1),\ (2),\ (3),\ (4),\ \ldots,\ (m),\ \ldots$$

benutzen und erkennen dann sofort, daß in dieser Reihe sich überhaupt keine Größe wiederholt. Wäre nämlich (m) und $(m+k)$ dieselbe Größe, so hätte man

$$(m+k) = (m) + (k) = (m),$$

also wäre im betrachteten Bereiche $(k) = 0$.

Daraus folgt aber, daß man das Zeichen (m) mit der ganzen Zahl m identifizieren kann; denn die durch das (gewöhnliche) Additions- und Multiplikationsgesetz festgelegten Eigenschaften der beiden Zeichen, die einzigen, von denen überhaupt Gebrauch gemacht wird, stimmen für beide überein. Genauer ausgedrückt ist:

$$(m) + (n) = (m+n);\quad (m)(n) = (mn);$$

ferner wird:

$$-1-1-\cdots = (-m) = -(m).$$

Wir können diese Tatsache noch folgendermaßen formulieren: Jeder holoide Bereich enthält den Bereich der rationalen und ganzen Zahlen, d. h. sämtliche ganze Zahlen, mit Einschluß der Null.

---

*) Die neugebildeten Worte holoid und orthoid sollen allgemeine Eigenschaften der Bereiche ausdrücken und ihrem Ursprung gemäß daran erinnern, daß die wesentlichen Eigenschaften des Bereichs der ganzen, resp. rationalen Zahlen erhalten bleiben. Für wirklich auftretende Bereiche wird die Gauß-Kroneckersche Terminologie festgehalten werden.

Man sagt: „Die Gleichung

$$\alpha\xi = \beta$$

ist in dem gegebenen Bereiche lösbar", wenn man eine Größe des Bereichs, ξ_1, angeben kann, für welche in der Tat $\alpha\xi_1 = \beta$ wird.

Der Bereich ist ein echter holoider Bereich, wenn man zwei bestimmte, von 0 verschiedene Größen α und β angeben kann, für welche die Gleichung $\alpha\xi = \beta$ nicht lösbar ist; der Bereich heißt orthoid oder unecht holoid, wenn im Bereiche immer eine Größe ξ_1 existiert, so daß $\alpha\xi_1 = \beta$ wird, wenn nur α von 0 verschieden ist.

Der Bereich der ganzen Zahlen ist demnach ein echter holoider Bereich; der Bereich der rationalen Zahlen ein unechter holoider (oder orthoider) Bereich; zu ihrer Bezeichnung werden wir die Symbole [1] und (1) benutzen.

Jeder holoide Bereich kann durch Hinzufügung („Adjunktion") neuer Größen zu einem orthoiden Bereiche erweitert werden.

Die neu hinzuzufügenden Größen können sogleich in der (vorläufig symbolischen) Form $\frac{\beta}{\alpha}$ geschrieben werden, wo α und β zwei beliebige Größen des ursprünglichen holoiden Bereichs sind und außerdem α von 0 verschieden sein soll; wenn noch festgesetzt wird, daß $\frac{\beta_1}{\alpha_1}$ und $\frac{\beta_2}{\alpha_2}$ dann und nur dann verschiedene Elemente sind, wenn $\alpha_1\beta_2 - \alpha_2\beta_1$ von 0 verschieden ist.

Eine solche Festsetzung ist bei der Definition des Bereichs unbedingt gestattet, und wird uns ein methodisch sehr wichtiges Hilfsmittel zur Bildung neuer Bereiche bieten. Sie führt jedoch — wie schon hier betont werden soll — zu der weiteren (arithmetisch-algebraischen) Forderung, jede Größe des erweiterten Bereichs in einer eindeutig bestimmten, kanonischen Form darzustellen.

Setzt man nun für den Bereich der „Größen" $\frac{\beta_1}{\alpha_1}$ das folgende Additions- und Multiplikationsgesetz fest:

$$\frac{\beta_1}{\alpha_1} + \frac{\beta_2}{\alpha_2} = \frac{\beta_1\alpha_2 + \beta_2\alpha_1}{\alpha_1\alpha_2}$$

$$\frac{\beta_1}{\alpha_1}\,\frac{\beta_2}{\alpha_2} = \frac{\beta_1\beta_2}{\alpha_1\alpha_2},$$

so erkennt man durch Wiederholung der Schlüsse der gemeinen Arithmetik, daß das Additions- und Multiplikationsgesetz ein „gewöhnliches“ ist; daß nach der oben gegebenen Definition nicht verschiedene oder „gleiche“ Größen, für einander gesetzt, das Resultat der Addition oder Multiplikation nicht ändern; daß ferner die Größe $\frac{0}{\alpha}$ die 0 und $\frac{\alpha}{\alpha}$ die absolute Einheit ist und schließlich die Größen $\frac{\beta}{1}$ genau die Eigenschaften der früheren Größen β besitzen. — Man kann also statt $\frac{\beta}{1}$ von nun an einfacher β schreiben und erhält als Lösung der Gleichung

$$\frac{\beta_1}{\alpha_1}\xi = \frac{\beta_2}{\alpha_2}$$

die Größe

$$\xi = \frac{\alpha_1 \beta_2}{\alpha_2 \beta_1},$$

wenn β_1 von Null verschieden ist; (α_1 und α_2 ist der Annahme nach nicht Null). Dabei wird $\frac{\beta}{\alpha}$, die Lösung der Gleichung

$$\alpha\xi = \beta,$$

das Resultat der Division von β durch α.

Der so gebildete Bereich heiße der dem ursprünglichen holoiden Bereich zugeordnete orthoide Bereich, der mit jenem zusammenfällt, wenn wir es mit einem unechten holoiden, also schon orthoiden Bereich zu thun hatten. Wir bezeichnen den ursprünglichen holoiden Bereich von nun an mit [A], den zugeordneten orthoiden Bereich mit (A). Jeder orthoide Bereich enthält — diesen Erörterungen entsprechend — den Bereich der rationalen Zahlen.

Teilbarkeit in holoiden Bereichen.

§ 5. Ist in dem vorgelegten holoiden Bereiche α irgend eine von 0 verschiedene Größe, und die Gleichung

$$\alpha\xi = \beta$$

lösbar, so heißt α ein Teiler (Divisor) von β und β ein Vielfaches von α.

In unecht holoiden Bereichen ist demnach jede Größe durch jede von 0 verschiedene Größe teilbar; man kann also auch in diesem Falle von Teilbarkeit sprechen, erhält aber dadurch keine weitere begriffliche Sonderung der im Bereiche enthaltenen Größen.

In einem echten holoiden Bereiche ist 0 die einzige Größe, die durch jede von 0 verschiedene Größe des Bereichs teilbar ist. Wäre γ eine solche und von 0 verschieden, so müßte sie auch durch γ^2 teilbar sein, und aus $\gamma = \gamma^2 \xi_1$ würde $1 = \gamma \xi_1$ folgen; γ wäre ein Teiler der absoluten Einheit. Nun gäbe es für eine beliebige, nur von 0 verschiedene Größe α eine Größe η, so daß

$$\alpha\eta = \gamma, \qquad \alpha\eta\xi_1 = 1,$$

also auch

$$\alpha(\eta\xi_1\beta) = \beta,$$

d. h. die Gleichung $\alpha\xi = \beta$ wäre immer lösbar, wenn α von 0 verschieden, und der Bereich kein echter holoider Bereich.

In einem echten holoiden Bereiche bilden demnach die Teiler einer von 0 verschiedenen Größe eine echte Teilmenge des Bereichs, d. h. eine solche, die auch nach Ausschluß der Null nicht sämtliche Größen des Bereichs erschöpft.

Insbesondere: Ist α kein Teiler von β, so ist auch $\mu\alpha$ kein Teiler von β.

Die beiden Elementargesetze der Teilbarkeit folgen unmittelbar aus der Definition. Sie lauten:

I. Ist γ durch β und β durch α teilbar, so ist auch γ durch α teilbar.

II. Sind β und γ durch α teilbar, so ist auch $\lambda\beta + \mu\gamma$ durch α teilbar, wo λ und μ beliebige Größen des Bereichs bedeuten.

Einheit heißt jede Größe des Bereichs, die ein Teiler der absoluten Einheit ist. Aus dieser Definition fließen unmittelbar die Folgerungen:

Jede Größe des Bereichs ist durch jede Einheit teilbar.

Das Produkt zweier Einheiten ist wieder eine Einheit.

Jeder Einheit ε_1 ist nämlich eine zweite ε_2 derart zugeordnet, daß $\varepsilon_1 \varepsilon_2 = 1$ wird. Also ist in der Tat

$$\alpha = \varepsilon_1 (\varepsilon_2 \alpha)$$

und auch:

$$(\varepsilon_1 \varepsilon_1')(\varepsilon_2 \varepsilon_2') = 1.$$

Zwei Größen des Bereichs heißen äquivalent (genauer absolut äquivalent im Gegensatz zur später einzuführenden relativen Äquivalenz), wenn jede von ihnen durch die andere teilbar ist.

Zwei Größen des Bereichs sind demnach dann und nur dann äquivalent, wenn jede von ihnen aus der andern durch Multiplikation mit einer Einheit entsteht.

Sind nämlich α und β äquivalent, so ist der Definition gemäß:

$$\alpha = \beta\mu, \qquad \beta = \alpha\nu.$$

Sie sind demnach zugleich 0 oder von 0 verschieden. Im letzteren Falle wird aber $\mu\nu = 1$. Also sind μ und ν Einheiten. Umgekehrt: Ist $\alpha = \beta\varepsilon_1$ und $\varepsilon_1 \varepsilon_2 = 1$, so folgt $\alpha\varepsilon_2 = \beta$.

Die Äquivalenz von α und β soll in Zeichen durch

$$\alpha \sim \beta$$

ausgedrückt werden. Die genauere Angabe des holoiden Bereichs, oder seiner Einheiten, ungefähr in der Form

$$\alpha \sim \beta, \qquad [A]$$

ist beinahe durchweg überflüssig, da die diesbezüglichen Annahmen im Laufe einer Untersuchung sich nicht ändern.

Der Äquivalenzbegriff ist eine Erweiterung des Gleichheitsbegriffs. Gleiche Größen sind auch äquivalent, und das Äquivalenzzeichen folgt denselben Grundgesetzen, wie das Gleichheitszeichen. Diese lauten:

I. Ist $\alpha \sim \beta$ und $\beta \sim \gamma$, so folgt auch $\alpha \sim \gamma$.

Soweit die Multiplikation in Betracht kommt, hat man in weiterer Analogie:

II. Ist $\alpha_1 \sim \beta_1$ und $\alpha_2 \sim \beta_2$, so folgt $\alpha_1\alpha_2 \sim \beta_1\beta_2$.

III. Ist $\alpha_1\alpha_2 \sim \beta_1\beta_2$ und $\alpha_2 \sim \beta_2$, so folgt $\alpha_1 \sim \beta_1$, wenn β_2 nicht 0 ist.

Die Richtigkeit beider Sätze erhellt unmittelbar, wenn man die Einheiten ε_1, ε_2, $\varepsilon_1\varepsilon_2 = \varepsilon_3$ einführt und das Äquivalenzzeichen durch das Gleichheitszeichen ersetzt. Z. B. im letzten Satze: Es ist $\alpha_1\alpha_2 = \beta_1\beta_2\varepsilon_3$, $\alpha_2 = \beta_2\varepsilon_2$; also $\alpha_1\beta_2\varepsilon_2 = \beta_1\beta_2\varepsilon_3$ und $\alpha_1\varepsilon_2 = \beta_1\varepsilon_3$, und schließlich wegen $\varepsilon_3 = \varepsilon_1\varepsilon_2$ auch $\alpha_1 = \beta_1\varepsilon_1$.

Man bemerke noch, daß $\alpha \sim 0$ immer $\alpha = 0$ nach sich zieht.

Im Bereiche der rationalen ganzen Zahlen sind $+1$ und -1 und nur diese Einheiten; die Äquivalenz bedeutet also in diesem Falle einfach, daß die beiden Zahlen gleich sind oder sich nur im „Vorzeichen" unterscheiden.

Im Bereiche der rationalen Zahlen, sowie in jedem unechten holoiden Bereiche sind in dieser Auffassung alle Zahlen, resp. alle Größen des Bereichs, mit Ausnahme der 0, Einheiten, und der Äquivalenzbegriff scheidet diese Größen in zwei Klassen, von denen die eine nur die 0, die andere sämtliche übrigen Größen umfaßt.

Ist α ein Teiler von β und weder $\alpha \sim 1$ noch $\alpha \sim \beta$, so heißt α ein echter Teiler von β.

Eine Größe des holoiden Bereichs heißt irreduzibel, wenn sie keinen echten Teiler besitzt.

Eine irreduzible Größe ist also entweder eine Einheit, oder eine echte irreduzible Größe, wenn sie eben keine Einheit ist.

Die echten irreduzibeln Größen in [1], dem Bereiche der rationalen und ganzen Zahlen, sind demnach die „natürlichen" Primzahlen 2, 3, 5, ...

Die Größe π heißt eine Prim-Größe, wenn sie nicht 0 und auch keine Einheit ist und irgend ein Produkt $\alpha\beta$ nur dann durch π teilbar ist, wenn schon α oder β eine durch π teilbare Größe ist.

Jede Primgröße π ist demnach irreduzibel; denn wenn $\pi = \pi_1 \pi_2$ und weder π_1 noch π_2 eine Einheit ist, so hätte man in $\pi_1 \pi_2$ ein durch π teilbares Produkt, dessen Faktoren nicht durch π teilbar sind. Wäre nämlich π_1 durch π teilbar, so müßte, da auch π durch π_1 teilbar ist, im Gegensatze zur Annahme π_2 eine Einheit sein.

Im Bereiche [1] fallen die Primgrößen mit den echten irreduzibeln Größen zusammen, sind also wieder die natürlichen Primzahlen. (S. Satz V des folgenden Paragraphen.)

Im allgemeinen ist zwar jede Primgröße irreduzibel, jedoch nicht jede echte irreduzible Größe eine Primgröße, wie schon das Beispiel am Ende des § 9 dieses Kapitels zeigen wird.

Der größte gemeinschaftliche Teiler.

§ 6. Sind α und β zwei Größen des holoiden Bereichs und δ eine solche Größe desselben Bereichs, daß α und β durch δ teilbar und auch jeder Teiler von α und β ein Teiler von δ ist, so heißt δ der größte gemeinschaftliche Teiler von α und β und soll durch (α, β) bezeichnet werden.

Jede Größe, die $\sim \delta$ ist, genügt mit δ zugleich diesen Bedingungen. Besitzen δ und δ' die für den größten gemeinschaftlichen Teiler von α und β geforderten Eigenschaften, so ist δ durch δ' und δ' durch δ teilbar, also $\delta \sim \delta'$. Die Bestimmung des größten gemeinschaftlichen Teilers ist demnach, insofern ein solcher überhaupt existiert, eine Äquivalenzbestimmung, und wir schreiben demgemäß:

$$(\alpha, \beta) \sim \delta .$$

Es ist insbesondere, wenn α beliebig, $(\alpha, 0) \sim \alpha$ und $(\alpha, \varepsilon) \sim 1$, wo ε eine Einheit bedeutet.

Der vorgelegte holoide Bereich heiße vollständig, wenn innerhalb des Bereiches sich zu jedem Größenpaare α und β eine Größe δ angeben läßt, die der größte gemeinschaftliche Teiler von α und β ist.

Nach elementaren Sätzen ist also z. B. der Bereich der rationalen und ganzen Zahlen ein vollständiger holoider Bereich.

Für vollständige holoide Bereiche gelten die folgenden grundlegenden Sätze:

I. Beliebig gewählte n Größen des Bereichs $\alpha_1, \ldots, \alpha_n$ besitzen einen größten gemeinschaftlichen Teiler δ in dem Sinne, daß δ ein Teiler sämtlicher α und umgekehrt jede Größe, die ein Teiler sämtlicher α, auch ein Teiler von δ ist.

Schreibt man wieder $(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim \delta$, so ist δ rekursiv auch durch

$$(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) = ((\alpha_1, \alpha_2, \ldots, \alpha_{n-1}), \alpha_n)$$

gegeben, was sich unmittelbar aus der Definition des größten gemeinschaftlichen Teilers ergibt; und auch:

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = ((\alpha_1, \ldots, \alpha_k), (\alpha_{k+1}, \ldots, \alpha_n)).$$

II. Ebenso erhellt unmittelbar, daß aus

$$\alpha_1 \sim \beta_1, \ \alpha_2 \sim \beta_2, \ \ldots, \ \alpha_n \sim \beta_n$$

auch

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim (\beta_1, \beta_2, \ldots, \beta_n)$$

folgt.

III. Man hat ferner

$$(\alpha_1\mu, \alpha_2\mu, \ldots, \alpha_n\mu) \sim (\alpha_1, \alpha_2, \ldots, \alpha_n)\mu.$$

Denn die links stehende Größe ist jedenfalls durch μ teilbar, also hat sie die Form $\delta\mu$. Soll aber $\delta\mu$ der größte gemeinschaftliche Teiler der Größen $\alpha_1\mu, \ldots, \alpha_n\mu$ sein, so muß einerseits jede Größe $\alpha\mu$ durch $\delta\mu$, also jedes α durch δ teilbar sein, und andrerseits, wenn δ' irgend ein Teiler sämtlicher α, auch $\delta\mu$ durch $\delta'\mu$, oder δ durch δ' teilbar sein. Es ist also in der That $\delta \sim (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Ein wichtiges Korollar dieses Satzes lautet:

Ist $(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim \delta$ und $\alpha_i \sim \delta\beta_i$, so folgt (mit Ausnahme des Falles, wo δ und also auch alle α gleich 0 sind) $(\beta_1, \beta_2, \ldots, \beta_n) \sim 1$.

Ist nämlich $(\beta_1, \beta_2, \ldots, \beta_n) \sim \delta'$, so folgt nach (III) auch

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \sim \delta\delta';$$

also $\delta\delta' \sim \delta$, und $\delta' \sim 1$.

IV. Für $(\mu, \nu) \sim 1$ hat man $(\alpha\mu, \nu) \sim (\alpha, \nu)$.

Der größte gemeinschaftliche Teiler von $\alpha\mu$ und ν ist jedenfalls auch ein Teiler von $\alpha\mu$ und $\alpha\nu$, also auch ein Teiler von $(\alpha\mu, \alpha\nu) \sim \alpha(\mu, \nu) \sim \alpha$. Demnach wird

$$(\alpha\mu, \nu) \sim (\alpha\mu, \alpha, \nu) \sim ((\alpha\mu, \alpha), \nu) \sim (\alpha, \nu).$$

Insbesondere folgt demnach aus $(\mu, \nu) \sim 1$ auch $(\mu^r, \nu^s) \sim 1$, wo r und s positive, ganze Zahlen bedeuten. Denn es ist dann

$$(\mu^r, \nu) \sim (\mu^{r-1}, \nu) \sim \cdots \sim (\mu, \nu) \sim 1,$$

und weiter:

$$(\mu^r, \nu^s) \sim (\mu^r, \nu^{s-1}) \sim \cdots \sim (\mu^r, \nu) \sim 1.$$

V. Ist π eine irreduzible Größe und $\alpha\beta$ durch π teilbar, so muß auch schon α oder β durch π teilbar sein; d. h. in einem vollständigen holoiden Bereiche ist jede irreduzible Größe eine Primgröße.

Wenn π irreduzibel, muß $(\gamma, \pi) \sim 1$ oder $(\gamma, \pi) \sim \pi$ sein. Wenn demnach α nicht durch π teilbar ist, wird $(\alpha, \pi) \sim 1$. Ist auch β nicht durch π teilbar, so ist auch $(\beta, \pi) \sim 1$ und demnach im Gegensatze zur Annahme $(\alpha\beta, \pi) \sim (\alpha, \pi) \sim 1$.

Beispiel: Die Bereiche $[\sqrt{-k}]$.

§ 7. Für Leser, die in dieser Darstellung zum erstenmal die allgemeineren Begriffsbildungen der Arithmetik und Algebra genauer kennen lernen, sollen — mit Unterbrechung der systematischen Darstellung — zur Unterstützung der Vorstellung schon hier Beispiele von holoiden Bereichen gegeben werden, die eine Erweiterung des Bereichs der ganzen Zahlen bieten, in denen aber die auf den größten gemeinschaftlichen Teiler bezüglichen Eigenschaften dieses einfachsten Typus nicht mehr erhalten bleiben, die insbesondere nicht mehr vollständig sind.

Die „Zahlen“ des zu definierenden Bereichs seien die Zahlenpaare (a, b), wo a und b gewöhnliche ganze Zahlen bedeuten. Die Addition und Multiplikation dieser Zahlen folgen den in den Formeln

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1)(a_2, b_2) = (a_1 a_2 - k b_1 b_2, a_1 b_2 + a_2 b_1)$$

ausgedrückten Gesetzen, wo k irgend eine feste positive ganze Zahl bedeutet.

Sowohl das Additions-, wie das Multiplikationsgesetz ist, wie man sich leicht überzeugt, ein „gewöhnliches".

Daß beide Gesetze associativ und kommutativ sind, tritt unmittelbar in Evidenz; ebenso der distributive Charakter der Multiplikation. Die Zahl $(0, 0)$ ist die einzige Null des Bereichs. Ist nämlich (a_1, b_1) von $(0, 0)$ verschieden, so folgt aus

$$(a_1, b_1)(a_2, b_2) = (a_1, b_1)(a_3, b_3) \tag{1}$$

oder den Gleichungen:

$$a_1 a_2 - k b_1 b_2 = a_1 a_3 - k b_1 b_3$$
$$a_1 b_2 + a_2 b_1 = a_1 b_3 + a_3 b_1,$$

die in anderer Form geschrieben

$$a_1 (a_2 - a_3) - k b_1 (b_2 - b_3) = 0 \tag{2}$$
$$b_1 (a_2 - a_3) + a_1 (b_2 - b_3) = 0$$

lauten, auch

$$a_2 - a_3 = 0, \qquad b_2 - b_3 = 0.$$

Betrachtet man nämlich $a_2 - a_3$, $b_2 - b_3$ als Unbekannte der linearen homogenen Gleichungen (2), so ergeben sich ihre Werte gleich Null, weil die aus den Koeffizienten gebildete Determinante $a_1^2 + k b_1^2$ den Annahmen nach von Null verschieden ist.

Der Bereich enthält die absolute Einheit; diese ist $(1, 0)$. Durch wiederholte Addition derselben entstehen die Zahlen $(2, 0), (3, 0), \ldots$; also niemals die Null.

Der aus den gesamten Zahlen (a, b) gebildete Bereich ist demnach ein holoider Bereich, und zwar ein echter holoider Bereich. Denn es ist z. B. die Gleichung

$$(2, 0)(x, y) = (1, 0)$$

unlösbar. Es müßte nach derselben

$$2x = 1, \qquad 2y = 0$$

sein. Es gibt also kein aus ganzen Zahlen gebildetes Paar (x, y), das jener Gleichung genügt.

Um nun die Zahlen des Bereichs möglichst einfach zu schreiben (und auch zu beschreiben), bemerke man zuerst, daß für die Zahlen $(m, 0)$, $(n, 0)$

$$(m, 0) + (n, 0) = (m + n, 0)$$
$$(m, 0)(n, 0) = (mn, 0)$$

ist, diese also genau den für gewöhnliche ganze Zahlen gültigen Gesetzen folgen. Also kann man innerhalb des Bereichs für $(m, 0)$ einfach m setzen, da die „Eigenschaften" beider Zahlen übereinstimmen, wenigstens insoweit, als sie für die gewöhnlichen ganzen Zahlen m festgesetzt sind.

Man bemerke ferner, daß:

$$(0, 1)(a, b) = (-kb, a),$$

insbesondere

$$(0, 1)(a, 0) = (0, a);$$

also

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + b(0, 1).$$

Wir wollen nun auch für $(0, 1)$ ein besonderes Zeichen wählen; mit Berücksichtigung des Umstandes, daß

$$(0, 1)(0, 1) = (-k, 0) = -k,$$

setzen wir, an die Zeichensprache der elementaren Algebra anknüpfend:

$$(0, 1) = \sqrt{-k}.$$

Dann wird schließlich die Zahl (a, b) mit $a + b\sqrt{-k}$ zu bezeichnen sein, und die additive und multiplikative Verknüpfung der Zahlen $a + b\sqrt{-k}$ geschieht „nach den gewöhnlichen Regeln der Algebra".

Den Bereich der Zahlen $a + b\sqrt{-k}$ bezeichnen wir mit dem Symbol $[\sqrt{-k}]$, wenn, wie hier vorausgesetzt, a und b dem Bereiche $[1]$ angehören.

Die Einheiten des Bereiches $[\sqrt{-k}]$ bestimmen sich

sehr einfach. Soll $x + y\sqrt{-k}$ eine Einheit sein, so muß eine zweite Zahl des Bereichs $u + v\sqrt{-k}$ existieren, so daß

$$(x + y\sqrt{-k})(u + v\sqrt{-k}) = 1$$

und also auch

$$(x - y\sqrt{-k})(u - v\sqrt{-k}) = 1$$

wird. Man hat demnach

$$(x^2 + ky^2)(u^2 + kv^2) = 1$$

und, da die Faktoren links gewöhnliche ganze Zahlen sind, die nicht negativ werden können, auch

$$x^2 + ky^2 = 1.$$

Hier scheiden sich die beiden Fälle $k = 1$ und $k > 1$.

Für $k = 1$ hat man entweder $x = \pm 1$, $y = 0$, oder $x = 0$, $y = \pm 1$; also enthält der Bereich $[\sqrt{-1}]$ die vier Einheiten: $1, -1, \sqrt{-1}, -\sqrt{-1}$. Es ist dies der Bereich der s. g. gewöhnlichen komplexen ganzen Zahlen, auf dessen weitere Behandlung hier nicht weiter eingegangen werden soll*).

Ist $k > 1$, so kann der Gleichung $x^2 + ky^2 = 1$ in gewöhnlichen ganzen Zahlen nur durch $x = \pm 1$, $y = 0$ genügt werden, und der Bereich $[\sqrt{-k}]$, wo $k > 1$, enthält nur die zwei Einheiten 1 und -1.

Um zu entscheiden, ob $u + v\sqrt{-k}$ ein Teiler von $a + b\sqrt{-k}$ ist, bemerke man, daß die notwendige und hinreichende Bedingung hierfür durch die Existenz zweier gewöhnlicher ganzer Zahlen x, y gegeben ist, für welche

$$a + b\sqrt{-k} = (u + v\sqrt{-k})(x + y\sqrt{-k}) \qquad (3)$$

ist. Dies ist der Fall, wenn das lineare Gleichungssystem

$$ux - kvy = a, \quad vx + uy = b$$

ein ganzzahliges Wertsystem als Lösung besitzt.

*) Siehe z. B. Bachmann, Kreisteilung, Leipzig, 1872. p. 150.

Die Reihe der Teiler einer Zahl $a + b\sqrt{-k}$ ist eine endliche und kann durch ein Verfahren bestimmt werden, das nach einer endlichen Anzahl von Schritten zum Abschluß gelangt. Denn mit (3) gilt auch immer

$$a - b\sqrt{-k} = (u - v\sqrt{-k})(x - y\sqrt{-k}); \qquad (4)$$

also ist auch

$$a^2 + kb^2 = (u^2 + kv^2)(x^2 + ky^2).$$

Die positive ganze Zahl $u^2 + kv^2$ ist demnach ein Teiler von $a^2 + kb^2$; sind also $d_i (i = 0, 1, \ldots, n)$ die positiven Teiler von $a^2 + kb^2$, so muß u, v einer der Gleichungen

$$u^2 + kv^2 = d_i \quad (i = 0, 1, \ldots, n)$$

genügen; da nun ferner einer jeden solchen Gleichung gemäß $u^2 \leqq d_i$, $v^2 \leqq d_i$ ist, so erhält man eine endliche Anzahl von Wertsystemen für u, v und hat dann nur für jede entsprechende Zahl $u + v\sqrt{-k}$ nach dem Vorgehenden zu entscheiden, ob sie ein Teiler von $a + b\sqrt{-k}$ ist.

§ 8. Wir gehen nun näher auf den Fall $k = 5$, d. i. auf den Bereich $[\sqrt{-5}]$ ein, dessen typische Bedeutung Dedekind*) zuerst gezeigt hat; er ist nämlich das einfachste Beispiel eines unvollständigen holoiden Bereichs.

Um dies zu erweisen, bestimmen wir die gesamten Teiler der Zahlen

$$3, 9, 1 - 2\sqrt{-5}, (1 - 2\sqrt{-5})^2 = -(19 + 4\sqrt{-5}),$$
$$3(1 - 2\sqrt{-5}).$$

Man hat z. B. im ersten Falle die Gleichungen $u^2 + 5v^2 = d$ aufzulösen, wo $d = 1, 3, 9$. Die ganzzahligen Wertsysteme, die sich hieraus ergeben, sind $(\pm 1, 0)$ im ersten und $(\pm 2, \pm 1), (\pm 3, 0)$ im dritten Falle, während der zweite Fall gar kein Wertsystem liefert.

---

*) Zahlentheorie, 4. Aufl. pag. 547.

Man erhält daher, vom Vorzeichen abgesehen, die Teiler

$$1 \text{ und } 3;$$

denn das Wertsystem $(\pm 2, \pm 1)$ gibt keinen Teiler. Es müßten nämlich noch z. B. aus

$$3 = (2 + \sqrt{-5})(x + y\sqrt{-5})$$

oder

$$2x - 5y = 3, \quad x + 2y = 0$$

sich dann ganzzahlige Werte von x und y ergeben. Dies ist aber für die einzige Lösung $\frac{2}{3}, -\frac{1}{3}$ nicht der Fall.

Hingegen hat man $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$.

Bei ähnlicher Ausführung der übrigen Rechnungen erhält man, vom Vorzeichen abgesehen, für die links stehenden Zahlen die folgenden Teilerreihen

3	$1, 3$
9	$1, 3, 2 \pm \sqrt{-5}, 9$
$1 - 2\sqrt{-5}$	$1, 1 - 2\sqrt{-5}$
$(1 - 2\sqrt{-5})^2$	$1, 1 - 2\sqrt{-5}, 2 - \sqrt{-5}, 2 + 3\sqrt{-5}, (1 - 2\sqrt{-5})^2$
$3(1 - 2\sqrt{-5})$	$1, 3, 1 - 2\sqrt{-5}, 2 - \sqrt{-5}, 4 - \sqrt{-5}, 3(1 - 2\sqrt{-5})$.

Hier sind demnach 9 und $3(1 - 2\sqrt{-5})$ zwei Zahlen, die keinen größten gemeinschaftlichen Teiler im festgesetzten Sinne des Wortes besitzen. Die gemeinschaftlichen Teiler beider Zahlen sind, vom Vorzeichen abgesehen:

$$1, 3 \text{ und } 2 - \sqrt{-5}.$$

Also müßte unter ihnen auch der größte gemeinschaftliche Teiler von 9 und $3(1 - 2\sqrt{-5})$ vorkommen, und dieser Teiler durch die übrigen teilbar sein; nun ist aber keine der

drei Zahlen durch die beiden andern teilbar, und damit auch unsre Behauptung erwiesen*).

In anderer, gleich auffallender Weise zeigt sich die „Unvollständigkeit" des Bereiches $[\sqrt{-5}]$ in dem Umstand, daß 3 und $1-2\sqrt{-5}$ außer der Einheit keinen gemeinsamen Teiler besitzen, wohl aber ihre Quadrate, die beide durch $2-\sqrt{-5}$ teilbar sind.

§ 9. Eine mit dem Vorhergehenden zusammenhängende Eigentümlichkeit des Bereiches $[\sqrt{-5}]$ besteht darin, daß die Gesamtheit der Zahlen in $[\sqrt{-5}]$, die durch 3 und $2-\sqrt{-5}$ teilbar sind, nicht durch die sämtlichen Vielfachen einer Zahl dargestellt werden kann.

Die Gesamtheit dieser Zahlen hat jedenfalls — wegen des Teilers 3 — die Form $3x+3y\sqrt{-5}$. Soll aber eine solche Zahl durch $2-\sqrt{-5}$ teilbar sein, so muß es gewöhnliche ganzzahlige Werte von u und v geben, die

$$3x+3y\sqrt{-5}=(2-\sqrt{-5})(u+v\sqrt{-5})$$

oder also

$$2u+5v=3x, \qquad -u+2v=3y$$

ergeben. Es sind demnach

$$u=\frac{2x-5y}{3}, \qquad v=\frac{x+2y}{3}$$

und auch

$$u-v+2y=\frac{x-y}{3}$$

gewöhnliche ganze Zahlen. Es folgt hieraus, wenn w wieder eine gewöhnliche ganze Zahl bedeutet:

$$x=y+3w;$$

*) Die beiden Aussagen, daß α und β keinen größten gemeinschaftlichen Teiler besitzen, und daß dieser gleich 1, haben also eine ganz verschiedene Bedeutung; was der in den Elementen vielfach gebrauchten ungenauen Ausdrucksweise gegenüber besonders bemerkt werden soll.

und, da dann u und v auch immer ganze Zahlen sind, wird die Gesamtheit der durch 3 und $2-\sqrt{-5}$ teilbaren Zahlen in $[\sqrt{-5}]$ durch

$$(9w+3y)+3y\sqrt{-5}=9w+3(1+\sqrt{-5})y$$

dargestellt, wo y und w beliebige gewöhnliche ganze Zahlen bedeuten.

Sollen diese sämtlich Vielfache einer bestimmten Zahl δ sein, so müßte dieses δ auch Teiler jener speziellen Zahlen sein, die man erhält, wenn man $w=1$, $y=0$ oder $w=1$, $y=-2$ setzt. Es wäre δ demnach ein Teiler von 9 und $3(1-2\sqrt{-5})$; also δ gleich 1, oder 3, oder $2-\sqrt{-5}$. Die gesamten Vielfachen dieser Zahlen geben aber immer auch Zahlen, die nicht durch 3 und $2-\sqrt{-5}$ teilbar sind, da ja schon 3 nicht durch $2-\sqrt{-5}$ und ebenso $2-\sqrt{-5}$ nicht durch 3 teilbar ist.

Der späteren Anwendung wegen sei noch insbesondere erwähnt, daß auch die Gesamtheit der Zahlen

$$3\alpha_1+(1-2\sqrt{-5})\alpha_2,$$

wo α_1 und α_2 beliebige Zahlen aus $[\sqrt{-5}]$ bedeuten, nicht mit der Gesamtheit der Vielfachen einer Zahl δ aus $[\sqrt{-5}]$ übereinstimmen kann.

Da unter jenen Zahlen sich auch 3 und $1-2\sqrt{-5}$ findet, so müßte δ ein gemeinsamer Teiler dieser Zahlen, also — vom Vorzeichen abgesehen — gleich 1 sein; und es müßte Werte von α_1 und α_2 geben, für welche

$$3\alpha_1+(1-2\sqrt{-5})\alpha_2=1$$

wird. Für dieselben Werte wäre aber, wenn man zum Quadrat erhebt,

$$9\alpha_1^2+6(1-2\sqrt{-5})\alpha_1\alpha_2+(1-2\sqrt{-5})^2\alpha_2^2=1.$$

Nun sind die Koeffizienten von α_1^2, $\alpha_1\alpha_2$ und α_2^2, wie die vorher ausgeführten Rechnungen zeigen, sämtlich durch $2-\sqrt{-5}$ teilbar. Gäbe es also dieser Bedingung entspre-

chende α_1 und α_2 in $[\sqrt{-5}]$, so wäre auch 1 durch $2-\sqrt{-5}$ teilbar, was nicht der Fall, da $2-\sqrt{-5}$ keine Einheit ist. Damit ist aber die oben aufgestellte Behauptung erwiesen.

Endlich sieht man, daß z. B. $2-\sqrt{-5}$ im Bereiche $[\sqrt{-5}]$ irreduzibel, aber keine Primgröße ist; denn weder 3 noch $1-2\sqrt{-5}$ sind durch diese Größe teilbar, wohl aber ihr Produkt.

Kongruenzbereiche und Modulsysteme.

§ 10. Aus dem vorgelegten holoiden Bereiche [A] wählen wir ein für allemal h bestimmte, von 0 verschiedene Größen $M_1, M_2, \ldots, M_h$, deren Inbegriff als Modulsystem $(M_1, M_2, \ldots, M_h)$ bezeichnet werden soll. Die Gesamtheit der Größen

$$\alpha_1 M_1 + \alpha_2 M_2 + \cdots + \alpha_h M_h,$$

wo $\alpha_1, \alpha_2, \ldots, \alpha_h$ beliebige, dem Bereiche [A] entnommene Größen sind, nennen wir einen (dem Bereiche [A] entstammenden) Kongruenzbereich, der durch das Modulsystem $(M_1, \ldots, M_h)$ bestimmt wird.

Das Modulsystem heißt nach der Anzahl der darin auftretenden Größen h-gliedrig, die in ihm enthaltenen Größen $M_1, M_2, \ldots$ sind seine Elemente.

Der Kongruenzbereich enthält nur dem Bereiche [A] angehörige Größen. Die Summe oder das Produkt zweier dem Kongruenzbereich angehöriger Größen gehört wieder dem Kongruenzbereiche an.

Die Gesamtheit der Größen des Bereichs [A] stimmt mit der Gesamtheit der Größen des Kongruenzbereichs dann und nur dann überein, wenn dieser die absolute Einheit enthält. Denn mit der 1 ist jede Größe aus [A] in der verlangten Form darstellbar.

Der Kongruenzbereich heißt echt, wenn er die absolute Einheit nicht enthält, also dann und nur dann, wenn er eine echte Teilmenge von [A] bildet.

Zwei Größen des Bereiches [A], z. B. λ und μ, heißen

kongruent in Bezug auf das Modulsystem $(M_1, M_2, \ldots, M_h)$, in Zeichen

$$\lambda \equiv \mu \pmod{M_1, M_2, \ldots, M_h},$$

wenn $\lambda - \mu$ dem durch das Modulsystem definierten Kongruenzbereiche angehört, oder also auch, wenn es in dem Bereiche [A] solche Größen α gibt, daß:

$$\lambda - \mu = \alpha_1 M_1 + \cdots + \alpha_h M_h$$

wird. Dieselbe Tatsache kann, wie unmittelbar ersichtlich, auch in der Form

$$\lambda - \mu \equiv 0 \pmod{M_1, M_2, \ldots, M_h}$$

ausgedrückt werden.

Der Kongruenzbegriff ist eine Erweiterung des Gleichheitsbegriffs. Gleiche Größen sind auch kongruent, und das Kongruenzzeichen folgt zum Teil denselben Grundgesetzen, wie das Gleichheitszeichen. Insbesondere:

I. Ist $\lambda \equiv \mu$ und $\mu \equiv \nu$, so folgt auch $\lambda \equiv \nu$.

II. Ist $\lambda_1 \equiv \lambda_2$ und $\mu_1 \equiv \mu_2$, so folgt auch $\lambda_1 \mu_1 \equiv \lambda_2 \mu_2$.

Dabei wird vorausgesetzt, daß das bestimmende Modulsystem immer dasselbe bleibt. Um z. B. den zweiten Satz zu beweisen, hat man nur die der Definition entsprechenden Tatsachen

$$\lambda_1 = \lambda_2 + \alpha_1 M_1 + \cdots + \alpha_h M_h$$
$$\mu_1 = \mu_2 + \beta_1 M_1 + \cdots + \beta_h M_h$$

ausführlich hinzuschreiben. Dann folgt unmittelbar:

$$\lambda_1 \mu_1 = \lambda_2 \mu_2 + \gamma_1 M_1 + \cdots + \gamma_h M_h.$$

Die Umkehrung dieses auf die Multiplikation bezüglichen Satzes ist nicht allgemein gültig. Der bezügliche genaue Satz lautet:

III. Ist $\lambda_1 \mu_1 \equiv \lambda_2 \mu_2$ und $\lambda_1 \equiv \lambda_2$, so folgt hieraus dann und nur dann für jede Größe μ_1 auch $\mu_1 \equiv \mu_2$, wenn es im Bereiche [A] eine Größe β gibt, für welche $\beta \lambda_1 \equiv 1$ wird.

Gibt es eine solche Größe, so ist wegen $\lambda_1 \equiv \lambda_2$ auch $\beta\lambda_2 \equiv \beta\lambda_1 \equiv 1$, ferner $\beta\lambda_1\mu_1 \equiv \beta\lambda_2\mu_2$; also auch $\mu_1 \equiv \mu_2$.

Daß es keine solche Größe β gibt, also die Gleichung

$$\beta\lambda_1 - \alpha_1 M_1 - \alpha_2 M_2 - \cdots - \alpha_h M_h = 1$$

nicht in der Weise lösbar ist, daß für $\beta, \alpha_1 \ldots, \alpha_h$ Größen des Bereichs [A] genommen werden, kann auch so gefaßt werden, daß das $(h+1)$-gliedrige Modulsystem $(\lambda_1, M_1, \ldots, M_h)$ einen echten Kongruenzbereich bestimmt; sämtliche Größen des durch das h-gliedrige Modulsystem $(M_1, \ldots, M_h)$ bestimmten Kongruenzbereichs sind in jenem enthalten; also bilden auch diese einen echten Kongruenzbereich. Wählt man nun für μ_1 und μ_2 zwei Größen, von denen die eine dem durch $(M_1, \ldots, M_h)$ bestimmten Kongruenzbereiche angehört, die andre nicht, was jetzt immer möglich, und λ_1, λ_2 so, daß beide $\equiv 0$ für $(M_1, \ldots, M_h)$, so wird auch $\lambda_1\mu_1 \equiv \lambda_2\mu_2$, ohne daß hieraus $\mu_1 \equiv \mu_2$ folgte.

Zwei Modulsysteme $(M_1, \ldots, M_h)$ und $(N_1, \ldots, N_k)$ ergeben in bestimmter Weise ein drittes, das sämtliche Elemente des ersten und zweiten enthält, $(M_1, \ldots, M_h, N_1, \ldots, N_k)$, wo aber der entsprechende Kongruenzbereich der Definition gemäß sich nicht ändert, wenn wir die eventuell wiederholt auftretenden Elemente nur einmal schreiben.

Ist nun

$$\lambda_1 \equiv \lambda_2 \pmod{M_1, \ldots, M_h} \quad \text{und} \quad \mu_1 \equiv \mu_2 \pmod{N_1, \ldots N_k},$$

so folgt unmittelbar auch:

$$\lambda_1 \equiv \lambda_2,\ \mu_1 \equiv \mu_2, \pmod{M_1, \ldots, M_h, N_1, \ldots, N_k}.$$

Dies gibt die folgende Erweiterung der Kongruenzsätze:

Ist $\lambda \equiv \mu \pmod{M_1, \ldots, M_h}$ und $\mu \equiv \nu \pmod{N_1, \ldots, N_k}$, so folgt auch $\lambda \equiv \nu \pmod{M_1, \ldots, M_h, N_1, \ldots, N_k}$.

Ist $\lambda_1 \equiv \lambda_2 \pmod{M_1, \ldots, M_h}$ und $\mu_1 \equiv \mu_2 \pmod{N_1, \ldots, N_k}$, so folgt auch $\lambda_1\mu_1 \equiv \lambda_2\mu_2 \pmod{M_1, \ldots, M_h, N_1, \ldots, N_k}$.

Ist $\lambda_1\mu_1 \equiv \lambda_2\mu_2 \pmod{M_1, \ldots, M_h}$ und $\lambda_1 \equiv \lambda_2 \pmod{N_1, \ldots, N_k}$, so folgt hieraus dann und nur dann

für jede Größe μ_1 auch $\mu_1 \equiv \mu_2$ (mod. $M_1, \ldots, M_h, N_1, \ldots, N_k$), wenn es im Bereiche [A] eine Größe β gibt, für welche

$$\beta\lambda_1 \equiv 1 \text{ (mod. } M_1, \ldots, M_h, N_1, \ldots, N_k).$$

Man kann den früher gegebenen Beweis wiederholen und hat nur zum Schluß $\lambda_1 = \lambda_2$ gleich einer Größe zu wählen, die $\equiv 0$ wird für das Modulsystem $(M_1, \ldots, M_h)$.

Wenn die beiden Modulsysteme $(M_1, \ldots, M_h)$ und $(N_1, \ldots, N_k)$ dieselben sind, erhält man die früher aufgestellten Sätze wieder.

§ 11. Das einfachste Beispiel dieser Begriffsbildungen wird durch die gewöhnliche Kongruenzbestimmung in den Elementen der Zahlentheorie geboten, wo Gauß zuerst den Ausdruck und das Zeichen der Kongruenz einführte, während die soeben gegebenen allgemeinen Begriffe Kronecker angehören*).

Zwei Zahlen des Bereiches [1] heißen dort kongruent in Bezug auf das eingliedrige Modulsystem (m) oder kürzer in Bezug auf den Modul m, wenn ihre Differenz durch m teilbar ist. Und so fort. Insbesondere definiert jede von 1 verschiedene ganze Zahl einen echten Kongruenzbereich, der aus sämtlichen Vielfachen von m und nur diesen besteht.

In diesem einfachsten Falle ist die Bildung weiterer mehrgliedriger Modulsysteme vollständig überflüssig. Sind nämlich $m_1, m_2, \ldots, m_h$ gewöhnliche ganze Zahlen, und d ihr größter gemeinschaftlicher Teiler, so gibt es stets ganze Zahlen $a_1, a_2, \ldots, a_h$ von der Beschaffenheit, daß

$$a_1 m_1 + \cdots + a_h m_h = d$$

wird. Der durch das Modulsystem $(m_1, \ldots, m_h)$ definierte Kongruenzbereich enthält also nur Vielfache von d und andrerseits alle Vielfache von d (denn es ist $kd = ka_1 m_1 + \cdots + ka_h m_h$), jener Bereich ist also mit dem durch den Modul (d) definierten Kongruenzbereich identisch.

*) Bis auf den — im Gebrauche sehr bequemen — Ausdruck „Kongruenzbereich".

Der Bereich der rationalen Zahlen (1) gibt zu keiner echten Kongruenzbestimmung Anlaß. Wäre in diesem $(r_1, r_2, \ldots, r_h)$ irgend ein Modulsystem, so ist schon die Gleichung $r_1 x \equiv 1$ in rationalen Zahlen lösbar, also auch alle Zahlen untereinander für jenes Modulsystem kongruent; der entsprechende Kongruenzbereich fällt also immer mit (1) zusammen.

Genau das gleiche gilt für jeden orthoiden Bereich.

Daß in höheren Bereichen die Verhältnisse nicht mehr so einfach sind, wie in [1], erhellt schon aus dem früher behandelten Beispiele des Bereiches $[\sqrt{-5}]$. Die Gesamtheit der Zahlen $3\alpha_1 + (1 - 2\sqrt{-5})\alpha_2$ ist nichts anderes, als der durch das zweigliedrige Modulsystem $(3, 1 - 2\sqrt{-5})$ bestimmte Kongruenzbereich, und wir haben eben (am Schluß des § 9) bewiesen, daß diese Bestimmung durch kein eingliedriges Modulsystem gegeben werden kann.

Die Wichtigkeit des Kongruenzbegriffs in arithmetischen Untersuchungen beruht auf der durch ihn gegebenen Klasseneinteilung der Größen des Bereichs [A], wenn wir nämlich alle mit einer bestimmten Größe kongruenten Größen oder, was damit gleichbedeutend, alle untereinander kongruenten Größen in eine Klasse zusammenfassen.

Relative Äquivalenz.

§ 12. Eine Teilmenge des vorgelegten holoiden Bereiches [A]

$$\pi_1, \pi_2, \ldots$$

die alle Einheiten in [A] enthält, die Null nicht enthält und endlich die Eigenschaft besitzt, daß das Produkt irgend zweier der Teilmenge angehöriger Größen wieder in dieser enthalten ist, heiße ein Äquivalenzbereich. Der Äquivalenzbereich heißt echt, wenn es eine Größe in [A] gibt, die von Null verschieden ist und die, mit irgend einer Größe des Äquivalenzbereichs multipliziert, niemals eine Größe dieses Äquivalenzbereichs ergibt.

Ein orthoider Bereich gibt daher niemals zur Bildung eines echten Äquivalenzbereichs Anlaß, da in diesem alle Größen, nach Ausschluß der Null, als Einheiten zu betrachten sind.

Geht man von [A], wie in § 4 dargelegt wurde, zu dem zugeordneten orthoiden Bereiche (A) über und bezeichnet den soeben charakterisierten Äquivalenzbereich mit Π, so bilden die gesamten Größen $\frac{\alpha}{\pi}$, wo α irgend eine Größe aus [A] und π irgend eine Größe aus Π ist, abermals einen holoiden Bereich, der mit $[A \mid \Pi]$ bezeichnet werden mag.

Der Bereich ist ein holoider, weil das Additionsgesetz

$$\frac{\alpha_1}{\pi_1} + \frac{\alpha_2}{\pi_2} = \frac{\alpha_1 \pi_2 + \alpha_2 \pi_1}{\pi_1 \pi_2}$$

und Multiplikationsgesetz

$$\frac{\alpha_1}{\pi_1} \frac{\alpha_2}{\pi_2} = \frac{\alpha_1 \alpha_2}{\pi_1 \pi_2}$$

ein gewöhnliches ist, ferner sowohl α wie π gleich der absoluten Einheit gesetzt werden können, und also der Bereich die Größen 1, 2, ... enthält, in deren Reihe sich die 0, wie unmittelbar ersichtlich, nicht findet.

Wenn [A] ein echter holoider Bereich und Π ein echter Äquivalenzbereich ist, und es ferner eine Größe γ in [A] gibt, die in keiner Größe des Äquivalenzbereichs als Teiler enthalten ist, — und nur in diesem Falle —, bilden die Größen $\frac{\alpha}{\pi}$ einen echten holoiden Bereich.

Jede Größe π ist in diesem Bereiche eine Einheit, weil $\pi \cdot \frac{1}{\pi} = 1$; also auch jede Größe $\frac{1}{\pi}$. Soll nun $\frac{\alpha}{\pi}$ eine Einheit sein, also z. B.

$$\frac{\alpha}{\pi} \frac{\alpha'}{\pi'} = 1$$

werden, so muß wegen $\alpha\alpha' = \pi\pi'$ jedenfalls α ein Teiler von $\pi\pi'$ in [A] sein. Die Einheiten des Bereiches $[A \mid \Pi]$ sind daher sämtliche Größen von der Gestalt $\frac{\varphi}{\pi}$, wo

φ Teiler irgend einer Größe aus Π sein muß, und nur diese.

Wählt man demnach für γ eine Größe aus $[A]$, die in Π nicht vorkommt, so wird die Gleichung $\gamma\xi = 1$ auch in dem neuen Bereiche unlösbar. Würde ihr $\xi = \frac{\beta}{\pi}$ genügen, so wäre $\gamma\beta = \pi$ und γ im Widerspruch zur Annahme ein Teiler von π in $[A]$.

Die Bedingungen des oben gegebenen Satzes sind damit als hinreichende erkannt. Daß sie auch notwendig sind, erkennt man in erster Linie daraus, daß, wenn für jede Größe γ des Bereichs $[A]$ eine Gleichung der Gestalt $\gamma\beta = \pi$ existiert, man für die Gleichung in $[A \mid \Pi]$

$$\frac{\gamma_1}{\pi'}\,\xi = \frac{\gamma_2}{\pi''}$$

nach Einführung der durch $\gamma_1\beta_1 = \pi_1$ definierten Größe unmittelbar die Lösung

$$\xi = \frac{\gamma_2\beta_1\pi'}{\pi_1\pi''}$$

findet. Dem ist nur noch die Bemerkung hinzuzufügen, daß, wenn der Äquivalenzbereich kein echter ist, jede Größe γ aus $[A]$ gewiß als Teiler einer Größe des Äquivalenzbereichs auftritt.

Jeder Äquivalenzbereich enthält die Einheiten des Bereichs $[A]$; diese allein bilden also den „kleinsten", dem $[A]$ entstammenden Aquivalenzbereich, der mit E bezeichnet werden soll. Man sieht unmittelbar, daß $[A \mid E]$ mit $[A]$ identisch ist.

Zwei Größen des Bereichs $[A]$, z. B. α und β, heißen in Bezug auf den Äquivalenzbereich Π relativ äquivalent, wenn es in Π zwei Größen π_1 und π_2 gibt, so daß $\pi_1\alpha = \pi_2\beta$ wird.

Dies soll in Zeichen durch

$$\alpha \sim \beta, \quad [A], \Pi$$

ausgedrückt werden, wo jedoch die genaue Angabe der Äquivalenzbestimmung, insofern sich diese im Laufe der Untersuchung nicht ändert, weggelassen werden kann.

Aus der soeben gegebenen Definition folgt unmittelbar, daß die früher (§ 5) festgestellten drei Grundgesetze der Äquivalenz auch jetzt gültig bleiben.

Fällt Π mit E zusammen, so wird aus der relativen die absolute Äquivalenz.

Die Wichtigkeit dieser Begriffsbestimmungen wird sich erst später zeigen; hier stehen uns nur ganz bedeutungslose Beispiele zur Verfügung. Man kann z. B. aus [1] alle Zahlen der Gestalt $\pm 2^k$ $(k = 0, 1, 2, \ldots)$ herausheben, wo dann zwei ganze Zahlen als relativ äquivalente zu bezeichnen sind, wenn die eine von ihnen durch Multiplikation mit einer Zahl der Gestalt $\pm 2^k$ in die andere übergeht. Der erweiterte Bereich $[\mathsf{A} \mid \Pi]$ besteht in diesem Falle aus allen Zahlen, deren Nenner eine Potenz von 2 ist.

Der Begriff der Äquivalenz kann von neuem erweitert werden, wenn wir in der Definition des Bereichs Π die Bedingung, daß Π alle Einheiten aus $[\mathsf{A}]$ enthalte, weglassen. Wir begnügen uns an dieser Stelle damit, dies einfach erwähnt zu haben.

Zweites Kapitel.

Holoiden Bereichen entstammende Formen.

Formen und ganze Funktionen.

§ 1. Es sei der holoide Bereich [A] vorgelegt. Aus den Größen dieses Bereichs und der neuen Unbestimmten x bilden wir die „Größen“

$$A_0 + A_1 x + A_2 x^2 + \cdots + A_m x^m,$$

wo $A_0, A_1, \ldots, A_m$ Größen des ursprünglichen Bereichs [A] bedeuten. Diese Größen fassen wir abermals zu einem Bereiche zusammen, indem wir, wenn eine zweite Größe

$$B_0 + B_1 x + B_2 x^2 + \cdots + B_n x^n$$

ist, als Summe, resp. Produkt der beiden die Größen

$$(A_0 + B_0) + (A_1 + B_1) x + (A_2 + B_2) x^2 + \cdots$$

und

$$A_0 B_0 + (A_0 B_1 + A_1 B_0) x + (A_0 B_2 + A_1 B_1 + A_2 B_0) x^2 + \cdots + A_m B_n x^{m+n}$$

bezeichnen, d. h. die Addition und Multiplikation nach den Regeln ausführen, die in den Elementen der Algebra für nach Potenzen von x geordnete Ausdrücke gegeben werden. Damit ist auch klargestellt, daß die ursprünglich gegebene Größe als Summe der Glieder $A_0, A_1 x, \ldots, A_m x^m$ betrachtet werden kann. Prinzipiell hätte diese Größe vor Festsetzung der Addition und Multiplikation eigentlich als Größenkomplex $(A_0, A_1, \ldots, A_m, x)$ geschrieben werden sollen, was aber nach dieser Festsetzung sogleich als überflüssige Komplikation erscheint.

Zwei solche Größen sind, ihrer Bildung entsprechend, dann und nur dann gleich, wenn die zu ihrer Darstellung verwendeten Größen des Bereichs [A], die s. g. Koeffizienten, der Reihe nach gleich sind,

$$A_0 = B_0,\ A_1 = B_1,\ \ldots,\ A_m = B_m,$$

und demnach auch ihre Anzahl in beiden Fällen dieselbe ist.

Man erkennt dann unmittelbar, daß die Gesamtheit der so gebildeten Größen einen echten holoiden Bereich bildet, und zwar auch dann, wenn der Bereich [A] ein unechter holoider, d. i. orthoider Bereich war. Denn die so definierten Größen besitzen ein gewöhnliches Additions- und Multiplikationsgesetz; der Bereich enthält ferner — mit allen Größen des Bereichs [A] — die absolute Einheit; und die aus dieser gebildete Reihe 1, 2, 3, ... enthält die Null nicht, da ja m und 0 der Definition nach verschiedene Größen sind. Daß der Bereich endlich ein echter holoider Bereich ist, erhellt daraus, daß die Gleichung

$$F\xi = 1$$

immer unlösbar ist, wenn F nicht dem engeren Bereiche [A] angehört oder — wie wir uns auch ausdrücken wollen — die Unbestimmte x wirklich enthält. Dann hat nämlich F die Gestalt

$$F = A_0 + A_1 x + \cdots + A_m x^m,$$

wo $m > 0$ und $A_m \neq 0$.

Soll $F\xi = 1$ sein, so ist keinesfalls $\xi = 0$, und ξ hätte also die Gestalt:

$$\xi = B_0 + B_1 x + \cdots + B_n x^n,$$

wo $n \geqq 0$ und $B_n \neq 0$. Dann ist aber

$$F\xi = A_0 B_0 + \cdots + A_m B_n x^{m+n},$$

wo $m + n > 0$ und $A_m B_n \neq 0$, und kann nicht $= 1$ werden, da diese Größe die Unbestimmte x wirklich enthält.

Der so gebildete Bereich soll kurz als $[A, x]$ bezeichnet werden.

§ 2. Es ist unmittelbar einzusehen, wie diese Begriffsbildung durch Einführung einer zweiten, dritten Unbestimmten und so fort weitergeführt werden kann.

Es seien die der Reihe nach einzuführenden Unbestimmten $x_1, x_2, \ldots, x_m$. Dann entsteht aus [A] zunächst der Bereich [A, x_1]; da dieser Bereich ein echter holoider Bereich ist, entsteht bei Hinzufügung der Unbestimmten x_2 ein neuer, erweiterter Bereich, der durch [A, x_1, x_2] bezeichnet werden kann und so fort, bis wir schließlich den Bereich

$$[\mathsf{A}, x_1, x_2, \ldots, x_m]$$

erhalten. Da auch in diesen Bereichen die Addition und Multiplikation nach den Regeln der elementaren Algebra geschieht, können in dem nach Potenzen von x_m geordneten Ausdrucke irgend einer Größe die Koeffizienten als Summen betrachtet werden, und man erhält, wenn die Multiplikationen wirklich ausgeführt werden, einen Ausdruck von der Gestalt

$$A_0 U_0 + A_1 U_1 + A_2 U_2 + \cdots + A_k U_k,$$

wo die Koeffizienten $A_0, A_1, \ldots$ dem ursprünglichen Bereiche [A] angehören und $U_0, U_1, \ldots, U_k$ verschiedene Potenzprodukte der Unbestimmten $x_1, x_2, \ldots, x_m$, d. h. Größen von der Gestalt

$$x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m}$$

bedeuten.

Diese Gestalt der Größen des Bereichs [A, $x_1, x_2, \ldots, x_m$] zeigt unmittelbar, daß die Reihenfolge, in der die Unbestimmten $x_1, \ldots, x_m$ zur Bildung dieses Bereichs verwendet werden, für diesen ganz gleichgültig ist und daß man auch in einem Schritte von A durch Hinzufügung des Systems von Unbestimmten $(x_1, x_2, \ldots, x_m)$ zu [A, $x_1, x_2, \ldots, x_m$] gelangen kann.

Man bezeichnet die Größen des Bereichs [A, $x_1, x_2, \ldots, x_m$] als (dem Bereiche [A] entstammende) Formen, oder auch ganze Funktionen der Unbestimmten $x_1, x_2, \ldots, x_m$.

Die beiden Benennungen sind mit zwei prinzipiell verschiedenen Auffassungen der neugebildeten Größen eng verknüpft.

In Wirklichkeit ist die Verwendung der Unbestimmten eine reine Übergangsbezeichnung. Aus zwei Größen des Bereichs

$$A_0 U_0 + \cdots + A_k U_k \quad \text{und} \quad B_0 U_0 + \cdots + B_l U_l$$

erhält man bei der Addition und Multiplikation eine dritte

$$C_0 U_0 + C_1 U_1 + \cdots + C_r U_r,$$

wo das Koeffizientensystem $(C_0, C_1, \ldots)$ in bestimmter Weise durch eine Reihe von Additionen und Multiplikationen aus den Koeffizientensystemen $(A_0, A_1, \ldots)$ und $(B_0, B_1, \ldots)$ zu bilden ist. Und dabei dienen die Potenzprodukte $U_0, U_1, \ldots$ nur dazu, das Gesetz, nach dem die verschiedenen Koeffizienten $A_0, A_1, \ldots, B_0, B_1, \ldots$ zu verwenden sind, in einfacher Weise zu charakterisieren; sie geben diesen Koeffizienten einen durch das Exponentensystem $(g_1, \ldots, g_m)$ ausgedrückten „Stellenwert". Man könnte demnach auch jene Formen als $(A_0, \ldots, A_k)$ bezeichnen, müßte aber dann ihr Additions- und Multiplikationsgesetz in sehr komplizierter Weise ausdrücken. Insofern nun jene Unbestimmten nur deshalb eingeführt werden, um die Verknüpfungen der neuen Größen in einfachster Weise beschreiben zu können, sprechen wir von Formen der Unbestimmten $x_1, \ldots, x_m$, in denen also die Koeffizienten $A_0, A_1, \ldots$ und ihre Stellenwerte $(g_1, \ldots, g_m)$ allein in Betracht kommen.

Der Ausdruck „ganze Funktion von $x_1, \ldots, x_m$" hat schon dem allgemeinen mathematischen Sprachgebrauche gemäß eine ganz andere Bedeutung. Dabei sind nämlich $x_1, \ldots, x_m$ in einer engeren Bedeutung des Wortes Unbestimmte, indem sie beliebige Größen des Bereichs [A], oder auch eines weiteren, [A] enthaltenden holoiden Bereiches [A'] bezeichnen, also beliebig bestimmte „Werte" annehmen können. Die ganze Funktion ist dann der Ausdruck eines speziellen Gesetzes, das aus den Größen $\xi_1, \ldots, \xi_m$, den Werten von $x_1, \ldots, x_m$, eine $m + 1^{\text{te}}$ Größe, den Wert der ganzen Funktion, bestimmt*).

*) Daß in der mathematischen Literatur der Ausdruck „Form" bisher meist nur für homogene ganze Funktionen benutzt wurde, konnte

Das Potenzprodukt $U_g = x_1^{g_1} x_2^{g_2} \dots x_m^{g_m}$ hat die Dimension $g_1 + g_2 + \cdots + g_m$ und den Grad g_i in Bezug auf x_i.

Die Form und auch die ganze Funktion

$$A_0 U_0 + A_1 U_1 + \cdots + A_k U_k$$

hat die Dimension n', resp. den Grad n_i in Bezug auf x_i, wenn n' resp. n_i die größte rationale ganze Zahl ist, die als Dimension resp. Grad in $U_0, U_1, \dots, U_k$ vorkommt, wobei natürlich nur diejenigen U zu zählen sind, die in dem Ausdruck der Form (ganzen Funktion) sich wirklich vorfinden, deren Koeffizient also nicht 0 ist.

Lexikographische Anordnung der Glieder einer Form.

§ 3. Für Formen mit einer Unbestimmten ist eine natürliche Reihenfolge der Glieder nach steigenden oder fallenden Potenzen dieser Unbestimmten unmittelbar gegeben. Die von Gauß*) gegebene konsequente Erweiterung dieses Ordnungsprinzips für Formen mit m Unbestimmten $x_1, x_2, \dots, x_m$ ist die folgende. Von zwei Gliedern

$$A_g x_1^{g_1} x_2^{g_2} \dots x_m^{g_m} \quad \text{und} \quad A_h x_1^{h_1} x_2^{h_2} \dots x_m^{h_m}$$

sei das erste das höhere, wenn $g_1 > h_1$; oder falls $g_1 = h_1$ ist, wenn $g_2 > h_2$; allgemein, falls $g_1 = h_1, g_2 = h_2, \dots, g_{i-1} = h_{i-1}$, wenn $g_i > h_i$. Da ähnliche Glieder (die dasselbe Potenzprodukt enthalten) schon als zusammengefaßt zu betrachten sind, gibt dies eine völlig bestimmte Anordnung vom niedrigsten bis zum höchsten Gliede.

---

keinen Grund dagegen abgeben, daß jene genaue begriffliche Sonderung, wie sie in Kroneckers Festschrift zuerst angeregt wurde, hier durchweg festgehalten wird. Eine Verwechslung der Bezeichnung ist kaum zu befürchten. Andrerseits ist aber nicht nur die schon in der Benennung enthaltene prinzipielle Scheidung der Bedeutung von hohem methodischen Werte, sondern auch die Durchführung einer klaren, einfachen Terminologie nur auf diesem Wege möglich. Man müßte sonst auf so kurze und treffende Bezeichnungen, wie z. B. ganze Form (wenn die Koeffizienten ganz sind), verzichten.

*) Demonstratio nova altera etc. Werke, Bd. III, pag. 36.

Die Höhe eines Gliedes, die in erster Reihe durch den Komplex der ganzen Zahlen $(g_1, g_2, \ldots, g_m)$ charakterisiert wird, kann aber, insofern unsere Betrachtungen zu gleicher Zeit nur eine bestimmte Anzahl von Formen umfassen, da jede von ihnen wieder nur aus einer bestimmten Anzahl von Gliedern besteht, auch durch eine einzige ganze Zahl festgelegt werden.

Zu diesem Zweck hat man nur eine positive ganze Zahl t zu wählen, die größer ist, als jeder Exponent g_i, der in den verschiedenen Gliedern der verschiedenen Formen vorkommt. Dann ist die Höhe des Gliedes $A_g x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m}$ durch die Zahl

$$g = g_1 t^{m-1} + g_2 t^{m-2} + \cdots + g_i t^{m-i} + \cdots + g_m \qquad (1)$$

vollständig bestimmt. Ist für ein anderes Glied

$$h = h_1 t^{m-1} + h_2 t^{m-2} + \cdots + h_i t^{m-i} + \cdots + h_m$$

und $g_1 = h_1, \ldots, g_{i-1} = h_{i-1}$, hingegen g_i und h_i verschieden, so haben $g - h$ und $g_i - h_i$, wie es der Aussage nach sein muß, gleiches Vorzeichen. Man hat

$$g - h = (g_i - h_i)\, t^{m-i} + (g_{i+1} - h_{i+1})\, t^{m-i-1} + \cdots + g_m - h_m$$

oder

$$\frac{g-h}{g_i - h_i} = t^{m-i} + \left(\frac{g_{i+1} - h_{i+1}}{g_i - h_i}\, t^{m-i-1} + \cdots + \frac{g_m - h_m}{g_i - h_i} \right).$$

Der in der Klammer stehende Ausdruck rechts ist, da alle $g_{i+1}, \ldots, g_m, h_{i+1}, \ldots, h_m$ nicht negativ und $< t$ sind, vom Vorzeichen abgesehen, nicht größer als

$$\frac{t-1}{|g_i - h_i|} \left(t^{m-i-1} + \cdots + 1 \right) = \frac{t^{m-i} - 1}{|g_i - h_i|},$$

also kleiner als t^{m-i}, und hieraus folgt in der That

$$\frac{g-h}{g_i - h_i} > 0.$$

Man sieht auch, daß die Darstellung von g in der Gestalt (1) nichts anderes ist, als die Darstellung in einem Zahlensystem mit der Grundzahl t, wo dann $g_1, g_2, \ldots, g_m$ einfach

die bei dieser Schreibweise zu verwendenden „Ziffern" sind. Die für die verschiedenen Glieder der Formen charakteristischen Höhenzahlen bilden demnach eine Reihe nicht negativer, ganzer Zahlen $0, g^{(1)}, g^{(2)}, \ldots$, die im allgemeinen Lücken enthält. Sei z. B. für t die Zahl $N+1$ gewählt, wenn alle Formen höchstens von der N^{ten} Dimension sind; dann wird das Ziffernsystem $(g_1, g_2, \ldots, g_m)$, wo $g_1 + g_2 + \cdots + g_m > N$, nicht auftreten können, da dieses einem Gliede von höherer als der N^{ten} Dimension entsprechen würde.

§ 4. Das soeben gewonnene Ordnungsprinzip gibt einen merkwürdigen und methodisch sehr wichtigen Zusammenhang zwischen Formen mit n Unbestimmten und solchen mit einer Unbestimmten*).

Wenn man nur solche Formen betrachtet, die von nicht höherer als der N^{ten} Dimension sind, so ist mit

$$F(x_1, x_2, \ldots, x_m) = \sum A_g x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m}$$

auch die Form

$$f(x) = \sum A_g x^g$$

völlig bestimmt, wenn man für t irgend eine Zahl gewählt hat, die $> N$, und g nach (1) bestimmt. Beschränkt man sich aber auf solche g, die bei diesen Bestimmungen als Höhenzahlen auftreten können, für die also im Zahlensystem mit der Grundzahl t die Summe der Ziffern nicht größer als N ist, so bestimmt sich auch umgekehrt aus $f(x)$ die Form $F(x_1, x_2, \ldots, x_m)$, da mit g dann auch die g_i gegeben sind.

Man hat daher eine gegenseitig eindeutige Beziehung zwischen den dem Bereiche [A] entstammenden Formen $F(x_1, \ldots, x_m)$ von nicht höherer als N^{ter} Dimension und den demselben Bereiche [A] entstammenden Formen $f(x)$, in denen nur solche Exponenten vorkommen, die in dem eben angegebenen Sinne Höhenzahlen sind.

*) Kronecker, Über die symmetrischen Funktionen, Berl. Mon.-Ber. 1880, pag. 938. Grundzüge einer arithmetischen Theorie der algebraischen Größen (= Festschrift) § 4. Crelle's Journal, Bd. 92.

Sind insbesondere $F_1, F_2, \ldots, F_k$ beliebige solche Formen und $F = F_1 F_2 \ldots F_k$ von der Dimension N, also F_i jedenfalls von nicht höherer Dimension, dann hat man auch

$$f = f_1 f_2 \cdots f_k,$$

wenn $f, f_1, f_2, \ldots, f_k$ die den $F, F_1, \ldots, F_k$ entsprechenden Formen der Unbestimmten x sind, da ähnlichen Gliedern immer wieder ähnliche Glieder entsprechen. Aus

$$\left(x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m}\right)\left(x_1^{h_1} x_2^{h_2} \ldots x_m^{h_m}\right) = x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}$$

folgt auch

$$x^g x^h = x^i,$$

und da der Multiplikationsprozeß demnach in beiden Fällen genau dieselben an den Koeffizienten auszuführenden Operationen verlangt, entspricht auch f dem F und erscheint mit dieser Form zugleich schon wohlgeordnet.

Die derivierten Formen.

§ 5. Setzt man in der Form $F(x_1, x_2, \ldots, x_m)$ an die Stelle von x_i die Summe $x_i + h_i$, wo h_i eine neue Unbestimmte bezeichnet, so kann man F nach Potenzen von h_i ordnen, wo dann die Koeffizienten abermals Formen der Unbestimmten $x_1, \ldots, x_m$ sind. Man nennt die hierbei als Koeffizient von h_i auftretende Form die (erste) Derivierte von F nach x_i und bezeichnet*) sie mit F'_{x_i} oder $\frac{\partial F}{\partial x_i}$.

*) Dieselbe Bildung tritt bekanntlich auch in den Elementen der Differentialrechnung auf, und es wird bequem sein, auch hier das Operationssymbol $\frac{\partial}{\partial x_i}$ zu verwenden, das aber natürlich als einheitliches Zeichen ohne Rücksicht auf seine geschichtliche oder analytische Bedeutung zu verstehen ist. Die Gesetze, denen die so definierte Operation gehorcht, müssen, wenn wir die Fundamentalgesetze der Algebra voll übersehen wollen, trotz ihres elementaren Charakters hier kurz entwickelt werden, schon um zu zeigen, daß es hierzu keines der Theorie fremden Hilfsmittels bedarf.

Man hat für das Monom Xx_i^k, wo X eine die Unbestimmte x_i nicht enthaltende Form ist, die Entwicklung

$$X(x_i + h_i)^k = Xx_i^k + kXx_i^{k-1}h_i + G_k h_i^2, \qquad (1)$$

die für $k = 1$ sich unmittelbar ergibt und — auch ohne Anwendung des Binomialsatzes, selbst in seiner einfachsten Gestalt — durch vollständige Induktion allgemein erhärtet wird. Ist die Entwicklung für irgend ein k gültig, so wird auch für $k + 1$, indem man $x_i + h_i$ als Factor hinzufügt:

$$X(x_i + h_i)^{k+1} = Xx_i^{k+1} + (k+1)Xx_i^k h_i + G_{k+1}h_i^2.$$

Somit ist, wenn X die Unbestimmte x_i nicht enthält:

$$\frac{\partial}{\partial x_i}(Xx_i^k) = kXx_i^{k-1}.$$

Da nun F in der Gestalt

$$F = X_0 + X_1 x_i + X_2 x_i^2 + \cdots + X_{n_i} x_i^{n_i}$$

geschrieben werden kann, wird:

$$F(\ldots, x_i + h_i, \ldots) = F(\ldots, x_i, \ldots) + \frac{\partial F}{\partial x_i}h_i + H_1 h_i^2.$$

Ist ähnlich für eine zweite Form

$$G(\ldots, x_i + h_i, \ldots) = G(\ldots, x_i, \ldots) + \frac{\partial G}{\partial x_i}h_i + H_2 h_i^2,$$

so ergeben sich durch Addition und Multiplikation dieser Entwicklungen die beiden Grundgesetze der Derivation:

$$\frac{\partial}{\partial x_i}(F + G) = \frac{\partial F}{\partial x_i} + \frac{\partial G}{\partial x_i} \qquad (I)$$

und

$$\frac{\partial}{\partial x_i}(FG) = F\frac{\partial G}{\partial x_i} + G\frac{\partial F}{\partial x_i}. \qquad (II)$$

Um in der Identität

$$F(\ldots, x_i + h_i, \ldots) = F_0 + F_1 h_i + F_2 h_i^2 + \cdots + F_{n_i} h_i^{n_i}$$

$$= \sum_{k=0}^{n_i} F_k h_i^k,$$

wo nach dem Vorhergehenden

$$F_0 = F,\ F_1 = \frac{\partial F}{\partial x_i}$$

ist, auch die übrigen als Koeffizienten von h_i^k auftretenden Formen als Derivierte zu bestimmen, setze man

$$x_i + h_i = z_i, \qquad h_i = z_i - x_i,$$

also

$$F(\ldots, z_i, \ldots) = \sum_{k=0}^{n_i} F_k (z_i - x_i)^k.$$

Wenn man nun allgemein die aus F durch l-malige Wiederholung des Derivationsprozesses entstehende Form die l^{te} Derivierte von F nach x_i (resp. z_i) nennt und mit $\frac{\partial^l F}{\partial x_i^{\,l}}$, resp. $\frac{\partial^l F}{\partial z_i^{\,l}}$ bezeichnet, so kann man rechts nach (1) die wiederholte Derivation nach z_i wirklich ausführen und hat:

$$\frac{\partial^l}{\partial z_i^{\,l}} F(\cdots, z_i, \cdots) = \sum_{k=l}^{n_i} k\,(k-1)\cdots(k-l+1)\,F_k (z_i - x_i)^{k-l},$$

also, wenn man in dieser Identität x_i statt z_i setzt, da rechts nur das Glied, in welchem $k = l$, nicht verschwindet:

$$\frac{\partial^l F}{\partial x_i^{\,l}} = l!\,F_l$$

und demnach die Entwicklung*)

$$F(\cdots, x_i + h_i, \cdots) = \sum_{k=0}^{n_i} \frac{1}{k!} \frac{\partial^k F}{\partial x_i^{\,k}} h_i^k. \tag{2}$$

§ 6. Wir setzen jetzt in der Form $F(x_1, x_2, \ldots, x_m)$ für alle $x_1, \ldots, x_m$ die Summen

$$x_1 + h_1,\ x_2 + h_2,\ \ldots,\ x_m + h_m,$$

wo $h_1, \ldots, h_m$ neue Unbestimmte sind, und ordnen

$$F(x_1 + h_1, \ldots, x_m + h_m)$$

nach den Potenzprodukten von $h_1, \ldots, h_m$.

---

*) wo noch die symbolischen Bezeichnungen $0! = 1$, $\frac{\partial^0 F}{\partial x_i^{\,0}} = F$ zu definieren sind.

Um den bei dieser Anordnung entstehenden Koeffizienten von $h_1^{k_1} h_2^{k_2} \dots h_m^{k_m}$ zu bestimmen, kann man auch folgendermaßen verfahren. Man setze zuerst nur für x_1 die Summe $x_1 + h_1$ und bestimme den Koeffizienten von $h_1^{k_1}$; in diesem Koeffizienten setze man wieder nur für x_2 die Summe $x_2 + h_2$ und bestimme den Koeffizienten von $h_2^{k_2}$ und so fort, bis schließlich für x_m die Summe $x_m + h_m$ gesetzt wird und in dem zuletzt erhaltenen Koeffizienten wieder der Koeffizient von $h_m^{k_m}$ bestimmt wird. Dies ergibt für den Koeffizienten von $h_1^{k_1} h_2^{k_2} \dots h_m^{k_m}$ den Ausdruck

$$\frac{1}{k_m!} \frac{\partial^{k_m}}{\partial x_m^{k_m}} \left(\frac{1}{k_{m-1}!} \frac{\partial^{k_{m-1}}}{\partial x_{m-1}^{k_{m-1}}} \left(\cdots \left(\frac{1}{k_1!} \frac{\partial^{k_1}}{\partial x_1^{k_1}} F \right) \cdots \right) \right),$$

oder

$$\frac{1}{k_m!\, k_{m-1}! \dots k_1!} \frac{\partial^{k_m}}{\partial x_m^{k_m}} \cdots \frac{\partial^{k_1} F}{\partial x_1^{k_1}}.$$

Die Bedeutung des so erhaltenen Resultats setzt die Vertauschbarkeit in der Reihenfolge der Operationen

$$\frac{\partial^{k_1}}{\partial x_1^{k_1}}, \dots, \frac{\partial^{k_m}}{\partial x_m^{k_m}}$$

unmittelbar in Evidenz; und auch die wiederholt auszuführenden Elementar-Operationen

$$\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_m}$$

geben, in beliebiger Reihenfolge ausgeführt, dasselbe Resultat, da ja nach dem Vorhergehenden für eine beliebige Form G

$$\frac{\partial}{\partial x_i} \frac{\partial G}{\partial x_g} = \frac{\partial}{\partial x_g} \frac{\partial G}{\partial x_i}$$

wird. Dementsprechend schreiben wir den so erhaltenen Coeffizienten von $h_1^{k_1} h_2^{k_2} \dots h_m^{k_m}$ kürzer:

$$\frac{1}{k_1!\, k_2! \dots k_m!} \frac{\partial^k F}{\partial x_1^{k_1} \partial x_2^{k_2} \dots \partial x_m^{k_m}} \qquad (k = k_1 + k_2 + \cdots + k_m)$$

und erhalten die Entwicklung:

$$\left.\begin{aligned} &F(x_1+h_1, x_2+h_2, \cdots, x_m+h_m) \\ &= \sum \frac{1}{k_1!\ldots k_m!} \frac{\partial^k F}{\partial x_1^{k_1}\ldots\partial x_m^{k_m}} h_1^{k_1}\cdots h_m^{k_m}, \end{aligned}\right\} \quad (3)$$

wo die Summation rechts sich auf alle Systeme von nicht negativen ganzen Zahlen $k_1, \ldots, k_m$ erstreckt, die der Bedingung

$$k = k_1 + k_2 + \cdots + k_m \leqq n'$$

genügen. Hier bedeutet n' die Dimension der Form F in den Unbestimmten $x_1, \ldots, x_m$.

Der polynomische Lehrsatz.

§ 7. Die Anwendung auf die spezielle Form

$$F = (x_1 + x_2 + \cdots + x_m)^n$$

ergibt den polynomischen Lehrsatz:

Es ist dann, wenn $k = k_1 + k_2 + \cdots + k_n$ gesetzt wird,

$$\frac{\partial^k F}{\partial x_1^{k_1}\partial x_2^{k_2}\ldots\partial x_m^{k_m}} = n(n-1)\cdots(n-k+1)(x_1+x_2+\cdots+x_m)^{n-k},$$

also

$$(x_1+h_1+x_2+h_2+\cdots+x_m+h_m)^n = \sum \frac{n(n-1)\cdots(n-k+1)}{k_1!\,k_2!\ldots k_m!}(x_1+x_2+\cdots+x_m)^{n-k} h_1^{k_1} h_2^{k_2}\ldots h_m^{k_m},$$

$$(k = k_1 + k_2 + \cdots + k_m \leqq n)$$

oder, wenn man die neue Unbestimmte

$$h_0 = x_1 + x_2 + \cdots + x_m$$

einführt und

$$n - k = k_0$$

setzt, wo dann

$$\frac{n(n-1)\cdots(n-k+1)}{k_1!\,k_2!\ldots k_m!} = \frac{n!}{k_0!\,k_1!\ldots k_m!}$$

wird, endlich

$$(h_0+h_1+\cdots+h_m)^n = \sum \frac{n!}{k_0!\,k_1!\ldots k_m!} h_0^{k_0} h_1^{k_1}\ldots h_m^{k_m} \quad (I)$$

$$(k_0+k_1+\cdots+k_m = n, \quad k_i = 0, 1, 2, \cdots, n).$$

Die auftretenden Koeffizienten, die s. g. Polynomialkoeffizienten, sind ihrer Entstehung nach positive, rationale und ganze Zahlen. Im einfachsten Falle ($m = 1$) schreiben wir die Binomialkoeffizienten auch in den Formen:

$$\frac{n!}{k_0!\,k_1!} = \binom{n}{k_0} = \frac{n(n-1)\cdots(n-k_0+1)}{k_0!}$$
$$= \binom{n}{k_1} = \frac{n(n-1)\cdots(n-k_1+1)}{k_1!},$$

wo die Identität beider Ausdrücke sich unmittelbar aus $k_0 + k_1 = n$ ergibt.

Man setze noch der Symmetrie wegen

$$\binom{n}{0} = 1$$

und bemerke die unmittelbar zu verifizierende Relation:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Homogene Formen.

§ 8. Eine Form heißt homogen, wenn ihre sämtlichen Glieder von derselben Dimension sind. Man kann in einer beliebigen Form alle Glieder gleicher Dimension in einer Teilsumme zusammenfassen und diese demgemäß:

$$F = \Phi_0 + \Phi_1 + \cdots + \Phi_r + \cdots + \Phi_n$$

schreiben, wo Φ_r eine homogene Form von der Dimension r ist. Dann ist bei Benutzung einer neuen Unbestimmten x_{m+1}

$$\Phi = \Phi_0 x_{m+1}^n + \Phi_1 x_{m+1}^{n-1} + \cdots + \Phi_r x_{m+1}^{n-r} + \cdots + \Phi_n$$

eine homogene Form n^{ter} Dimension der Unbestimmten $x_1, \ldots x_m, x_{m+1}$, welche die F entsprechende homogene Form heißt.

Die Anzahl der Glieder, die in Φ_n vorkommen können, ist die Anzahl der verschiedenen Formen von der Gestalt

$$x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} \qquad (k_1 + \cdots + k_m = n),$$

das ist die Anzahl der verschiedenen nicht negativen, ganzzahligen Wertesysteme, die der Bedingung

$$k_1 + \cdots + k_m = n$$

genügen. Ist m und n gegeben, so bestimmt sich diese Anzahl durch eine endliche Reihe von Versuchen und kann demnach vorläufig als $\{m, n\}$ bezeichnet werden. Man hat unmittelbar

$$\{m, 0\} = 1$$
$$\{m, 1\} = m$$

und allgemein

$$\{m, n\} = \{m - 1, n\} + \{m, n - 1\},$$

da in der Summe rechts zuerst die Anzahl jener Glieder steht, in denen z. B. x_m nicht vorkommt, und dann die Anzahl jener Glieder, in denen x_m vorkommt, nichts anderes ist als die Anzahl der Glieder in einer homogenen Form $n - 1^{\text{ter}}$ Dimension der Unbestimmten $x_1, \ldots, x_m$.

Daraus folgt durch vollständige Induktion als Anzahl der möglichen Glieder in $\Phi_n(x_1, \ldots, x_m)$

$$\{m, n\} = \binom{m + n - 1}{n},$$

die für $m = 1$ und $n = 0$ oder 1 richtig ist. Setzt man diese als erwiesen voraus, wenn $m + n$ kleiner als eine bestimmte Zahl N ist, so wird

$$\{m, n+1\} = \{m-1, n+1\} + \{m, n\}$$
$$= \binom{m+n-1}{n+1} + \binom{m+n-1}{n} = \binom{m+n}{n+1};$$

also ist die Formel auch gültig, wenn $m + n = N$, und damit auch als allgemein gültig erwiesen.

Die Anzahl der möglichen Glieder in der nicht homogenen Form n^{ter} Dimension $F(x_1, \ldots, x_m)$ ist

$$\{m + 1, n\} = \binom{m + n}{n},$$

denn sie stimmt mit der Anzahl der Glieder in Φ überein. Zählt man diese als die Summe der Gliederanzahl in Φ_0, Φ_1, $\ldots$, Φ_n, so erhält man die Relation:

$$\binom{m+n}{n} = 1 + \binom{m}{1} + \cdots + \binom{m+r-1}{r} + \cdots + \binom{m+n-1}{n}.$$

§ 9. Eine Form $F(x_1, x_2, \ldots, x_m)$ ist dann und nur dann homogen und von der n^{ten} Dimension, wenn

$$F(tx_1, tx_2, \ldots, tx_m) = t^n F(x_1, x_2, \ldots, x_m).$$

Daß eine homogene Form Φ_r in der Tat einer solchen Relation genügt, ist unmittelbar klar. Ist umgekehrt $F = \sum_{i=1}^{k} \Phi_i$, also

$$F(tx_1, tx_2, \ldots, tx_m) = \sum_{i=1}^{k} \Phi_i(tx_1, tx_2, \ldots, tx_m),$$

so wird ferner, wenn F der angegebenen Bedingung genügt, auch

$$t^n F(x_1, x_2, \ldots, x_m) = \sum_{i=1}^{k} t^i \Phi_i(x_1, x_2, \ldots, x_m),$$

und wenn man die Koeffizienten gleicher Potenzen von t auf beiden Seiten vergleicht,

$$\Phi_i = 0 \quad (i \neq n), \quad \Phi_n = F.$$

Es sei noch schließlich die folgende von Euler herrührende Formelreihe für eine homogene Form n^{ter} Dimension $\Phi(x_1, x_2, \ldots, x_m)$ erwähnt:

$$\left.\begin{aligned} & n(n-1)\cdots(n-k+1)\,\Phi \\ &= \sum_{i_k=1}^{m} \cdots \sum_{i_2=1}^{m} \sum_{i_1=1}^{m} x_{i_1} x_{i_2} \cdots x_{i_k} \frac{\partial^k \Phi}{\partial x_{i_1} \partial x_{i_2} \ldots \partial x_{i_k}}. \end{aligned}\right\} \quad \text{(I)}$$

Der einfachste Fall $k = 1$

$$n\Phi = \sum_{i=1}^{m} x_i \frac{\partial \Phi}{\partial x_i} \quad \text{(Ia)}$$

wird durch Ausführung der rechts angedeuteten Operationen unmittelbar als richtig erwiesen. Die allgemeine Formel der Reihe wird durch vollständige Induktion verifiziert. Man setzt die Richtigkeit der Formel für ein bestimmtes k voraus; dann ist jede k^{te} Derivierte von Φ eine homogene Form $n - k^{\text{ter}}$ Dimension, für welche nach (Ia)

$$(n-k) \frac{\partial^k \Phi}{\partial x_{i_1} \partial x_{i_2} \ldots \partial x_{i_k}} = \sum_{i_{k+1}=1}^{m} x_{i_{k+1}} \frac{\partial^{k+1} \Phi}{\partial x_{i_1} \ldots \partial x_{i_k} \partial x_{i_{k+1}}}$$

wird. Setzt man dies in (I) ein, so entsteht unmittelbar die entsprechende Formel für $k + 1$.

Man bemerke noch die für irgend welche Größen bestehende Identität

$$\sum_{i_k=1}^{m} \cdots \sum_{i_2=1}^{m} \sum_{i_1=1}^{m} c_{i_1} c_{i_2} \cdots c_{i_k} = (c_1 + c_2 + \cdots + c_m)^k,$$

die für $k = 1$ unmittelbar in Evidenz tritt und durch vollständige Induktion als allgemein richtig erwiesen wird, wenn man mit

$$\sum_{i_{k+1}=1}^{m} c_{i_{k+1}} = c_1 + c_2 + \cdots + c_m$$

multipliziert. Die Eulerschen Formeln können demzufolge in der unmittelbar verständlichen, oft bequemen symbolischen Gestalt

$$\left.\begin{aligned} &n(n-1)\cdots(n-k+1)\,\Phi \\ &= \left(x_1 \frac{\partial}{\partial x_1} + x_2 \frac{\partial}{\partial x_2} + \cdots + x_m \frac{\partial}{\partial x_m}\right)^k \Phi \end{aligned}\right\} \qquad \text{(II)}$$

geschrieben werden.

Die elementaren symmetrischen Formen.

§ 10. Wenn man in irgend einer Form F an Stelle der Unbestimmten $z_1, z_2, \ldots, z_r$ je die Unbestimmten $z_{i_1}, z_{i_2}, \ldots, z_{i_r}$ setzt, wo $i_1, i_2, \ldots, i_r$ die Zahlen $1, 2, \ldots, r$ in irgend einer beliebigen Reihenfolge bedeuten, oder wenn man, wie wir uns kurz ausdrücken, die Substitution

$$\begin{pmatrix} z_1 & z_2 & \ldots & z_r \\ z_{i_1} & z_{i_2} & \ldots & z_{i_r} \end{pmatrix}$$

auf die Form F ausübt, so wird dadurch eigentlich eine gewisse gesetzmäßige Vertauschung der Koeffizienten der Form bewirkt.

Eine Form F heißt eine symmetrische Form der Unbestimmten $z_1, z_2, \ldots, z_r$, wenn immer

$$F(z_{i_1}, z_{i_2}, \ldots, z_{i_r}) = F(z_1, z_2, \ldots, z_r)$$

ist, die Form sich also bei Ausübung sämtlicher Substitutionen der betrachteten Art nicht ändert.

Die Form F kann außer $z_1, \ldots, z_r$ noch andere Unbestimmte $u_1, u_2, \ldots, u_s$ enthalten, auf welche sich die obige Aussage nicht bezieht. Ordnet man die in $z_1, z_2, \ldots, z_r$ symmetrische Form S nach Potenzprodukten der $u_1, \ldots, u_s$:

$$S(z_1, z_2, \ldots, z_r, u_1, u_2, \ldots, u_s) = \sum' S_j(z_1, z_2, \ldots, z_r)\, U_j,$$

so ist auch

$$S(z_{i_1}, z_{i_2}, \ldots, z_{i_r}, u_1, u_2, \ldots, u_s) = \sum S_j(z_{i_1}, z_{i_2}, \ldots, z_{i_r})\, U_j$$

und, da der Definition nach die linken Seiten gleich sind, auch

$$S_j(z_{i_1}, z_{i_2}, \ldots, z_{i_r}) = S_j(z_1, z_2, \ldots, z_r),$$

also ist jeder Koeffizient in der Entwicklung nach den Potenzprodukten der $u_1, \ldots, u_s$ eine symmetrische Form der Unbestimmten $z_1, z_2, \ldots, z_r$.

§ 11. Für die allgemeine Theorie der symmetrischen Formen sind die s. g. elementaren symmetrischen Formen von grundlegender Bedeutung. Diese entstehen aus der Form

$$P^{(k)}(z) = (z - x_{k+1})(z - x_{k+2}) \cdots (z - x_m), \qquad \text{(I)}$$

die kurz als $P^{(k)}(z)$ bezeichnet werden soll. Es ist unmittelbar ersichtlich, daß diese als Produkt geschriebene Form symmetrisch in $x_{k+1}, x_{k+2}, \ldots, x_m$ ist. Es wird also, wenn man nach Potenzen von z ordnet, auch jeder Koeffizient diese Eigenschaft besitzen, und die Gleichung

$$P^{(k)}(z) = z^{m-k} - \mathfrak{f}_1^{(k)} z^{m-k-1} + \mathfrak{f}_2^{(k)} z^{m-k-2} - \cdots$$
$$+ (-1)^r \mathfrak{f}_r^{(k)} z^{m-k-r} + \cdots + (-1)^{m-k} \mathfrak{f}_{m-k}^{(k)}$$

$\mathfrak{f}_1^{(k)} \ldots \mathfrak{f}_{m-k}^{(k)}$ als „elementare symmetrische Formen der Unbestimmten $x_{k+1}, \ldots, x_m$“ definieren.

Die explizite Gestalt

$$\mathfrak{f}_r^{(k)} = \sum x_{i_{k+1}} x_{i_{k+2}} \cdots x_{i_r},$$

(wo sich die Summation auf alle verschiedenen Kombinationen, d. h. nicht bloß durch die Reihenfolge verschiedene Systeme $i_{k+1}, \ldots, i_r$ erstreckt, die aus den Zahlen $k+1, k+2, \ldots, m$ gebildet werden können), ist ohne Schwierigkeit zu erkennen, wird aber eigentlich nicht benutzt.

Im Falle $k = 0$, wo sämtliche x in den zu bildenden Formen auftreten, soll, um eine möglichst einfache Bezeichnung zu erhalten, der obere Index ganz weggelassen werden. Endlich schreiben wir noch, um bequemer zusammenfassen zu können, $\mathfrak{f}_0^{(k)} = 1$. Dann wird

$$P^{(k)}(z) = \sum_{r=0}^{m-k} (-1)^r \mathfrak{f}_r^{(k)} z^{m-k-r},$$

$$P(z) = \sum_{r=0}^{m} (-1)^r \mathfrak{f}_r z^{m-r}.$$

Die Transformation $z = u + x_{k+i}$ ergibt

$$P^{(k)}(u + x_{k+i}) = \sum_{r=0}^{m-k} (-1)^r \mathfrak{f}_r^{(k)} (u + x_{k+i})^{m-k-r}$$

und also links unmittelbar den Faktor u. Es muß also auch rechts, wenn man nach Potenzen von u ordnet, das von u freie Glied 0 sein. Dies ergibt die fundamentale Identität:

$$\sum_{r=0}^{m-k} (-1)^r \mathfrak{f}_r^{(k)} x_{k+i}^{m-k-r} = P^{(k)}(x_{k+i}) = 0 \qquad \text{(II)}$$

$$(i = 1, 2, \ldots, m-k),$$

insbesondere für $k = 0$ auch:

$$\sum_{r=0}^{m} (-1)^r \mathfrak{f}_r x_i^{m-r} = P(x_i) = 0, \qquad (i = 1, 2, \ldots, m) \qquad \text{(IIa)}$$

Diese Relationen ergeben, wie wir zeigen wollen, die Identität:

$$\left| x_{k+i}^{m-k-j} \right|_{(i,j=1,\ldots,m-k)} = \prod_{r,s} (x_r - x_s), \qquad \text{(III)}$$

$$\begin{pmatrix} r, s = k+1, \ldots, m, \\ r < s. \end{pmatrix}$$

oder, wie wir uns auch ausdrücken können, die explizite

Berechnung der links stehenden Determinante*). Insbesondere ist für $k = m - 2$ in der Tat

$$\begin{vmatrix} x_{m-1} & 1 \\ x_m & 1 \end{vmatrix} = x_{m-1} - x_m.$$

Wir werden also für den allgemeinen Beweis wieder die vollständige Induktion anwenden können. Die i^{te} Zeile der zu berechnenden Determinante ist ausführlich geschrieben:

$$x_{k+i}^{m-k-1}, x_{k+i}^{m-k-2}, \ldots, x_{k+i}^{m-k-j}, \ldots, x_{k+i}, 1.$$

Multipliziert man demnach die Elemente der zweiten, ..., j^{ten}, ..., vorletzten und letzten Spalte der Reihe nach mit

$$-\mathfrak{f}_1^{(k+1)}, \ldots, (-1)^{j-1}\mathfrak{f}_{j-1}^{(k+1)}, \ldots, (-1)^{m-k-2}\mathfrak{f}_{m-k-2}^{(k+1)}, \\ (-1)^{m-k-1}\mathfrak{f}_{m-k-1}^{(k+1)}$$

und addiert zur ersten, so wird in der so transformierten Determinante das Element c_{i1} gleich

$$\sum_{r=0}^{m-k-1}(-1)^r \mathfrak{f}_r^{(k+1)} x_{k+i}^{m-k-1-r} = P^{(k+1)}(x_{k+i}),$$

also in der ersten Zeile:

$$c_{11} = P^{(k+1)}(x_{k+1}) = (x_{k+1} - x_{k+2})(x_{k+1} - x_{k+3}) \cdots (x_{k+1} - x_m).$$

Weiter ist in den übrigen Zeilen $c_{i1} = 0$ $(i \neq 1)$. Die Determinante zerfällt demnach in das Produkt von $P^{(k+1)}(x_{k+1})$ und der aus $x_{k+2}, \ldots, x_m$ ähnlich gebildeten Determinante, für welche (III) als erwiesen angenommen wird, und man hat demnach

$$\left| x_{k+i}^{m-k-j} \right|_{(i,j=1,\ldots,m-k)} = P^{(k+1)}(x_{k+1}) \prod_{\substack{r,s \\ r<s}} (x_r - x_s) \qquad \begin{pmatrix} r, s = k+2, \ldots, m \\ r < s \end{pmatrix},$$

*) Wo irgend möglich, werden wir, um die Anschauung zu erleichtern, Determinanten immer so beschreiben, daß c_{ij} das in der i^{ten} Zeile und j^{ten} Spalte stehende Element bezeichnet. Die Determinanten werden der Raumersparnis wegen meist nicht in ausführlicher Form hingeschrieben, was aber der weniger geübte Leser leicht ergänzen kann.

wo die rechte Seite unmittelbar als der rechten Seite in (III) gleich erkannt wird.

Man bezeichnet das Quadrat jenes Differenzenproduktes auch mit $\Delta(x_{k+1}, \ldots, x_m)$ oder Δ_k; demzufolge schreiben wir das soeben erhaltene Resultat in der neuen, häufig gebrauchten Gestalt:

$$\left| x_{k+i}^{m-k-j} \right|^2 = \Delta(x_{k+1}, \ldots, x_m) = \Delta_k; \qquad (i, j = 1, 2, \ldots, m-k). \qquad \text{(IIIa)}$$

§ 12. Dieselbe Methode führt zur Auswertung der folgenden allgemeineren Determinante

$$m(m-1)\ldots(m-e+1)^{\text{ten}} \text{ Grades:}$$

$$\left| x_{i_1}^{j_1} x_{i_2}^{j_2} \ldots x_{i_e}^{j_e} \right|, \qquad \begin{pmatrix} i_1, i_2, \ldots, i_e = 1, 2, \ldots, m \\ i_r \neq i_s \\ 0 \leqq j_r \leqq m-r \end{pmatrix},$$

wo, um die Anschauung zu fixieren*), in der ersten Zeile $i_1 = 1$, $i_2 = 2, \ldots, i_e = e$ sei und die Elemente der ersten Zeile nach ihrer Höhe als Potenzprodukte der x geordnet sein mögen. Es ist insbesondere $c_{11} = x_1^{m-1} x_2^{m-2} \ldots x_e^{m-e}$, und da nach diesen Festsetzungen das Element c_{11} die ganze Determinante charakterisiert, werden wir diese auch mit

$$\left[x_1^{m-1} x_2^{m-2} \ldots x_e^{m-e}\right]$$

bezeichnen. Dabei muß natürlich die Reihenfolge der Systeme $(i_1, i_2, \ldots, i_e)$ fixiert sein, und insofern dies nicht geschieht, bleibt das Vorzeichen der Determinante unbestimmt.

Um diese Determinante zu berechnen, schreiben wir sie in Gestalt einer eigentümlichen symbolischen Determinante; und zwar sei die erste Zeile dieser symbolischen Determinante:

$$x_1^{m-1}\left[x_2^{m-2} \ldots x_e^{m-e}\right], x_1^{m-2}\left[x_2^{m-2} \ldots x_e^{m-e}\right], \ldots,$$
$$x_1\left[x_2^{m-2} \ldots x_e^{m-e}\right], \left[x_2^{m-2} \ldots x_e^{m-e}\right],$$

*) Die zur Verwendung gelangenden Systeme $(i_1, \ldots, i_e)$ sind nichts anderes als die e-gliedrigen Variationen der Elemente $1, \ldots, m$ ohne Wiederholung.

während die i^{te} Zeile aus der ersten durch Vertauschung von x_1 und x_i entstehen möge. Die Determinante besteht also jetzt aus m Zeilen und Spalten. Dabei bedeutet jedes einzelne Element das ganze Schema der Elemente jener durch den Klammerausdruck bezeichneten Determinante, die noch jedes einzeln mit dem vorstehenden Faktor zu versehen sind. Jedes Element ist also das Symbol eines Determinantenschemas vom Grade $(m-1)\cdots(m-e+1)$ und, wenn man die Elemente in der angegebenen Weise nebeneinander reiht, entsteht, wie unmittelbar einzusehen, die zu berechnende Determinante.

Da nun weiter der Klammerausdruck in jeder Zeile durchweg derselbe ist, wird jene identische Transformation, bei der man die mit irgend einem Faktor multiplizierten Elemente einer Spalte zu den entsprechenden Elementen einer andern Spalte hinzufügt, auch jetzt den Wert der Determinante nicht ändern; denn auch in der wirklichen Determinante werden wieder nur die mit gewissen Faktoren multiplizierten Elemente einer ganzen Reihe von Spalten zu den entsprechenden Elementen einer anderen Spaltenreihe addiert.

Wenn man also die $2^{\text{te}}\ldots$ bis m^{te} Spalte der symbolisch geschriebenen Determinante mit

$$-\mathfrak{f}_1^{(1)}, \mathfrak{f}_2^{(1)}, \cdots, (-1)^{m-1}\mathfrak{f}_{m-1}^{(1)}$$

multipliziert und zur ersten Spalte addiert, wird nach (I) und (II)

$$c_{11} = P^{(1)}(x_1)\left[x_2^{m-2}\ldots x_e^{m-e}\right], \quad c_{i1} = 0 \qquad (i>1).$$

Wenn man nun in der so transformierten Determinante wieder die 3te bis m^{te} Spalte mit

$$-\mathfrak{f}_1^{(2)}, \mathfrak{f}_2^{(2)}, \cdots, (-1)^{m-2}\mathfrak{f}_{m-2}^{(2)}$$

multipliziert und zur zweiten addiert, erhält man

$$c_{22} = P^{(2)}(x_2)\left[x_2^{m-2}\ldots x_e^{m-e}\right]_{(1,2)}, \quad c_{i2} = 0 \qquad (i>2),$$

wo die der Klammer zugefügte Bezeichnung (1, 2) die Vertauschung von x_1 und x_2 fordert.

In derselben Weise fortfahrend, transformiert man allgemein die r^{te} Spalte so, daß

$$c_{rr} = P^{(r)}(x_r)\left[x_2^{m-2} \dots x_e^{m-e}\right]_{(1,r)}, \quad c_{ir} = 0 \qquad (i > r).$$

Dann ist aber die gesuchte Determinante nichts anderes als das Produkt der Determinanten

$$\left[x_2^{m-2} \dots x_e^{m-e}\right]_{(1,r)} \qquad (r = 1, 2 \dots m),$$

wenn noch jedes Element der betreffenden Determinante mit $P^{(r)}(x_r)$, oder also, da die betr. Determinante vom Grade $(m-1)\dots(m-e+1)$ ist, diese selbst mit $(P^{(r)}(x_r))^{(m-1)\dots(m-e+1)}$ multipliziert wird. Demnach ist

$$\left.\begin{aligned} &\left[x_1^{m-1} x_2^{m-2} \dots x_e^{m-e}\right] = \\ &= \left[x_1^{m-1}\right]^{(m-1)\dots(m-e+1)} \prod_{r,s}^{m} \left[x_2^{m-2} \dots x_e^{m-e}\right]_{(1,r)} \end{aligned}\right\}, \qquad \text{(IV)}$$

da

$$P^{(1)}(x_1)\, P^{(2)}(x_2) \dots P^{(m-1)}(x_{m-1}) = \prod_{r,s}(x_r - x_s)$$

$$\begin{pmatrix} r, s = 1, 2, \dots, m \\ r < s \end{pmatrix}$$

wird und dieses Differenzenprodukt nach der eingeführten Schreibweise mit $\left[x_1^{m-1}\right]$ bezeichnet werden kann.

Dies führt unmittelbar zu folgender allgemeiner Bestimmung der fraglichen Determinante:

$$\left[x_1^{m-1} x_2^{m-2} \dots x_e^{m-e}\right] = \pm \left[x_1^{m-1}\right]^{\varphi(m,\,e)} \qquad \text{(V)}$$

$$\varphi(m, 1) = 1, \quad \varphi(m, 2) = 2m - 3,$$

$$\varphi(m, e) = \frac{e(2m-e-1)}{2}(m-2)(m-3)\cdots(m-e+1) \quad (e>2).$$

Das Vorzeichen hängt natürlich von der für die Zeilen der Determinante bestimmten Reihenfolge ab. Die vollständige Induktion wird (V) als allgemein richtig erweisen, nachdem für $e = 1$ die beiden Seiten auch formell übereinstimmen. Allgemein ist, wenn (V) für irgend ein $e - 1$ als richtig vorausgesetzt wird,

$$\left[x_2^{m-2} \cdots x_e^{m-e}\right]_{(1,r)} = \pm X_r^{\varphi(m-1,\,e-1)},$$

wo X_r das Differenzenprodukt der Unbestimmten $x_1, x_2, \ldots, x_m$ mit Ausschluß von x_r bedeutet. Da $x_r - x_s$ in jedem X_i, mit Ausschluß von X_r und X_s, einmal vorkommt, wird

$$\prod_{r=1}^{m}\left[x_2^{m-2} \cdots x_e^{m-e}\right]_{(1,r)} = \pm\left[x_1^{m-1}\right]^{(m-2)\,\varphi(m-1,\,e-1)}$$

und demnach $\left[x_1^{m-1} x_2^{m-2} \cdots x_e^{m-e}\right]$ gleich

$$\pm\left[x_1^{m-1}\right]^{(m-1)\ldots(m-e+1)\,+\,(m-2)\,\varphi(m-1,\,e-1)}.$$

Hieraus erhellt*) die in

$$\varphi(m, e) = (m-1)\cdots(m-e+1) + (m-2)\,\varphi(m-1, e-1)$$

enthaltene rekursive Bestimmung von $\varphi(m, e)$, die in den einfachsten Fällen

$$\varphi(m, 2) = 2m - 3, \qquad \varphi(m, 3) = 3(m-2)^2$$

in Übereinstimmung mit (V) ergibt, während allgemein für $e > 3$

$$\varphi(m, e) = (m-1)\cdots(m-e+1)$$
$$+ (m-2)\,\frac{(e-1)(2m-e-2)}{2}\,(m-3)\cdots(m-e+1)$$
$$= \left(m - 1 + \frac{(e-1)(2m-e-2)}{2}\right)(m-2)\cdots(m-e+1)$$

sich als identisch mit der entsprechenden Bestimmung in (V) ergibt.

Man erhält schließlich das Quadrat jener Determinante als Potenz von $\Delta(x_1, x_2, \ldots, x_m)$ in der Formel:

$$\left[x_1^{m-1} x_2^{m-2} \ldots x_e^{m-e}\right]^2 = \Delta^{\varphi(m,\,e)}, \qquad \text{(VI)}$$

wo Δ für $\Delta(x_1, x_2, \ldots, x_m)$ gesetzt ist.

---

*) Wenn man schon festgestellt hat, daß die fragliche Determinante eine Potenz jenes Differenzenproduktes ist, so folgt der Wert der ganzen Zahl $\varphi(m, e)$ — nach einer mündlichen Mitteilung meines Kollegen, Herrn G. Rados — unmittelbar daraus, daß die Dimension der Determinante, als Form der Unbestimmten $x_1, \ldots, x_m$, direkt ausgerechnet werden kann.

Die reduzierten Formen.

§ 13. Nach einem von Kronecker*) herrührenden grundlegenden Satze ist jede Form F der Unbestimmten $x_1, x_2, \ldots, x_m$ gleich einer — und nur einer — „reduzierten" Form, d. h. gleich einem Ausdruck

$$\sum_{(j)} \mathfrak{F}_j x_1^{j_1} x_2^{j_2} \ldots x_{m-1}^{j_{m-1}} \qquad (0 \leqq j_r \leqq m-r;\ r = 1, \ldots, m-1),$$

wo**) $\mathfrak{F}_j$ eine „Form der elementaren symmetrischen Formen" $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$ ist, oder — mit andern Worten — die Gestalt

$$\mathfrak{F}_j = \sum_{(g)} C_g \mathfrak{f}_1^{g_1} \mathfrak{f}_2^{g_2} \ldots \mathfrak{f}_m^{g_m}$$

besitzt, und hier wieder C_g eine „rationale und ganze" lineare Form der Koeffizienten der ursprünglichen Form $F(x_1, \ldots, x_m) = \sum_h A_h x_1^{h_1} x_2^{h_2} \ldots x_m^{h_m}$ bedeutet, d. h.

$$C_g = \sum_{(h)} k_h A_h$$

wird, wo die k_h rationale und ganze Zahlen sind.

Für eine Unbestimmte verliert der Satz seinen Inhalt, bleibt aber gleichwohl richtig, da dann einfach $x_1 = \mathfrak{f}_1$ ist.

Für zwei Unbestimmte x_1 und x_2 ist die angegebene Umgestaltung unmittelbar auszuführen. Man setzt zuerst $x_2 = \mathfrak{f}_1 - x_1$ und kann dann mittels der Identität

$$x_1^2 - \mathfrak{f}_1 x_1 + \mathfrak{f}_2 = 0,$$

die auch

$$x_1^k - \mathfrak{f}_1 x_1^{k-1} + \mathfrak{f}_2 x_1^{k-2} = 0 \qquad (k \geqq 2)$$

---

*) „Über die verschiedenen Sturmschen Reihen". Mon.-Ber. Berl. Ak. Februar, 1873. Werke, Bd. I, pag. 323.

**) Der Ausdruck, der aus $F(x_1, \ldots, x_m)$ dadurch entsteht, daß für die Unbestimmten $x_1, \ldots, x_m$ die Größen $X_1, \ldots, X_m$ gesetzt werden, also $F(X_1, \ldots, X_m)$, heiße kürzer eine Form der Größen $X_1, \ldots, X_m$. Eine Form heißt rational und ganz, wenn ihre Koeffizienten rationale und ganze Zahlen sind.

geschrieben werden kann, x_1^k, wo $k \geqq 2$, formell aus der Darstellung entfernen und damit unmittelbar zur reduzierten Form gelangen.

Die vollständige Induktion führt nun allgemein zur Aufstellung der reduzierten Form.

Ordnet man F nach Potenzen von x_1, so wird jeder Koeffizient eine Form der $m-1$ Unbestimmten $x_2, \ldots, x_m$ und kann demnach in der Gestalt

$$\sum_{(j)} \mathfrak{F}_j^{(1)} x_2^{j_2} \ldots x_{m-1}^{j_{m-1}} \qquad (0 \leqq j_r \leqq m-r)$$

geschrieben wevden, wo $\mathfrak{F}_j^{(1)}$ eine Form der elementaren symmetrischen Formen $\mathfrak{f}_1^{(1)}, \ldots, \mathfrak{f}_{m-1}^{(1)}$ ist und die Koeffizienten rationale und ganze lineare Formen der Koeffizienten der vorgelegten Form sind. Nun entspringen aus der Identität

$$(z - x_1)\left(z^{m-1} - \mathfrak{f}_1^{(1)} z^{m-2} + \mathfrak{f}_2^{(1)} z^{m-3} - \ldots\right)$$
$$= z^m - \mathfrak{f}_1 z^{m-1} + \mathfrak{f}_2 z^{m-2} - \ldots$$

die weiteren Identitäten:

$$x_1 + \mathfrak{f}_1^{(1)} = \mathfrak{f}_1$$
$$x_1 \mathfrak{f}_1^{(1)} + \mathfrak{f}_2^{(1)} = \mathfrak{f}_2$$
$$\ldots\ldots\ldots\ldots$$
$$x_1 \mathfrak{f}_{r-1}^{(1)} + \mathfrak{f}_r^{(1)} = \mathfrak{f}_r$$
$$\ldots\ldots\ldots\ldots$$
$$x_1 \mathfrak{f}_{m-2}^{(1)} + \mathfrak{f}_{m-1}^{(1)} = \mathfrak{f}_{m-1}$$

oder auch

$$\mathfrak{f}_1^{(1)} = \mathfrak{f}_1 - x_1$$
$$\mathfrak{f}_2^{(1)} = \mathfrak{f}_2 - \mathfrak{f}_1 x_1 + x_1^2$$
$$\ldots\ldots\ldots\ldots$$
$$\mathfrak{f}_r^{(1)} = \mathfrak{f}_r - \mathfrak{f}_{r-1} x_1 + \mathfrak{f}_{r-2} x_1^2 - \mathfrak{f}_{r-3} x_1^3 + \cdots + (-1)^r x_1^r$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\mathfrak{f}_{m-1}^{(1)} = \mathfrak{f}_{m-1} - \mathfrak{f}_{m-2} x_1 + \mathfrak{f}_{m-3} x_1^2 - \cdots + (-1)^{m-1} x_1^{m-1},$$

nach deren Benutzung an die Stelle von $\mathfrak{F}_j^{(1)}$ eine Form von $x_1, \mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$ mit Koeffizienten tritt, die den früheren Angaben entsprechen. Entfernt man schließlich x_1^{m+k}, wo $k \geqq 0$, mittels der Identität

$$x_1^m - \mathfrak{f}_1 x_1^{m-1} + \mathfrak{f}_2 x_1^{m-2} - \cdots + (-1)^m \mathfrak{f}_m = 0,$$

so erhält man die reduzierte Form mit den angegebenen Eigenschaften.

Daß nur eine solche reduzierte Form existieren kann, ist im Falle einer Unbestimmten unmittelbar evident und kann für den allgemeinen Fall wieder durch vollständige Induktion bewiesen werden.

Die angegebenen Operationen, die zur reduzierten Form führen, sind nämlich eindeutig umkehrbar. Führt man in der reduzierten Form wieder zuerst x_1 statt $\mathfrak{f}_m$ ein, sodann $\mathfrak{f}_1^{(1)}, \ldots, \mathfrak{f}_{m-1}^{(1)}$ statt $\mathfrak{f}_1, \ldots, \mathfrak{f}_{m-1}$ und ordnet endlich nach Potenzen von x_1, so erhält man wieder F_1 nach Potenzen von x_1 geordnet, mit Koeffizienten von der Gestalt

$$\sum_{(j)} \mathfrak{F}_j^{(1)} x_2^{j_2} \ldots x_{m-1}^{j_{m-1}} \qquad (0 \leqq j_r \leqq m - r).$$

Wären nun zwei reduzierte Formen für F vorhanden, so erhielte man eine zweite Darstellung von F, in welcher die Koeffizienten der einzelnen Potenzen von x_1

$$\sum_{(j)} \overline{\mathfrak{F}}_j^{(1)} x_2^{j_2} \ldots x_{m-2}^{j_{m-1}}$$

wären, und diese müßten jedenfalls gleich den entsprechenden früher gefundenen sein. Dann sind sie aber mit diesen identisch, denn beide sind reduzierte Formen der $m - 1$ Unbestimmten $x_2, \ldots, x_m$.

Die beiden reduzierten Formen für F, die wir als verschieden annahmen, mußten also doch identisch gleich sein.

§ 14. Ist die zu reduzierende Form symmetrisch in Bezug auf $x_{k+1}, \ldots, x_m$ — sie möge dann mit $S^{(k)}(x_1, \ldots, x_m)$ bezeichnet werden —, so fallen in der reduzierten Form

alle jene Glieder fort, in denen $x_{k+1}, \ldots, x_m$ explizite vorkommen würde.

Um dies klarzustellen, ordnen wir die $S^{(k)}$ entsprechende reduzierte Form nach Potenzprodukten der Unbestimmten $x_{k+1}, \ldots, x_m$ und gelangen dadurch zu einer Identität von der Gestalt

$$\Phi_h x_{k+1}^{h_{k+1}} \cdots x_{m-1}^{h_{m-1}} + \cdots + \Phi_j x_{k+1}^{j_{k+1}} \cdots x_{m-1}^{j_{m-1}} + \cdots + \Phi_0 - S^{(k)} = 0,$$

wo die Koeffizienten Φ nur mehr $x_1, \ldots, x_k, \mathfrak{f}_1, \ldots, \mathfrak{f}_m$ enthalten.

Setzt man für $x_{k+1}, \ldots, x_m$ in dieser Identität $x_{r_{k+1}}, \ldots, x_{r_m}$, wo $r_{k+1}, \ldots, r_m$ irgend eine Permutation der Zahlen $k+1, \ldots, m$ bedeuten, so bleibt die Identität bestehen, während weder eine der Formen Φ, noch der Annahme nach $S^{(k)}$ sich ändern. Es entstehen also $(m-k)!$ Relationen, die als homogene lineare Gleichungen zur Bestimmung von $\ldots \Phi_j, \ldots \Phi_0 - S^{(k)}$ aufgefaßt werden können; auch diese Größen sind in der Anzahl $(m-k)!$ vorhanden.

Die Determinante des Systems, nämlich

$$\left[x_{k+1}^{m-k-1}\, x_{k+2}^{m-k-2} \ldots x_{m-1}\right]$$

ist aber wieder eine von 0 verschiedene Größe, also

$$\Phi_j = 0 \quad (j > 0); \quad \Phi_0 = S^{(k)},$$

was zu beweisen war.

Für $k = 0$ ergibt sich hieraus der Hauptsatz von der Darstellbarkeit der symmetrischen Formen durch die elementaren symmetrischen Formen:

Jede symmetrische Form $S(x_1, \ldots, x_m)$ ist darstellbar als Form der elementaren, symmetrischen Formen $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$ mit Koeffizienten, die rationale und ganze, homogene lineare Formen der in S auftretenden Koeffizienten sind.

Diese Darstellung wird prinzipiell durch die Berechnung der reduzierten Form gegeben; eine Reihe von speziellen Methoden, auf die wir hier nicht eingehen, dient zur Abkürzung

des Verfahrens und ergibt zugleich die durch $S(x_1, \ldots, x_m)$ bedingten Eigenschaften der entsprechenden reduzierten Form.

Eine weitere wichtige Folgerung aus dem Vorhergehenden besteht in dem Satze:

Die elementaren symmetrischen Formen $\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_m$ sind voneinander unabhängig. Mit dieser kurzen Ausdrucksweise soll folgende Tatsache bezeichnet sein: Eine Identität von der Gestalt

$$\sum_g A_g \mathfrak{f}_1^{g_1} \mathfrak{f}_2^{g_2} \ldots \mathfrak{f}_m^{g_m} = 0$$

kann nur dann stattfinden, wenn sämtliche Koeffizienten A_g gleich 0 sind, wie immer auch der holoide Bereich [A] gewählt sei, dem die Koeffizienten A_g angehören. Der Natur der Sache nach wird dabei nur vorausgesetzt, daß $x_1, x_2, \ldots, x_m$ neue Unbestimmte, also nicht etwa dem Bereiche [A] angehörige Größen sind. Wir werden diesen weittragenden Satz weiterhin als Gaußsches Prinzip bezeichnen; Gauß hat zuerst seine fundamentale Wichtigkeit für die Beweismethoden der Algebra gezeigt*).

Eine solche Identität, in welcher nicht sämtliche A_g verschwinden, ergäbe nämlich eine reduzierte Form zur Darstellung der Null, die von derjenigen, in welcher sämtliche A_g gleich Null sind, die also selbstverständlich die Null ergibt, verschieden wäre; eine solche zweite reduzierte Form kann aber, wie bewiesen wurde, nicht existieren.

§ 15. In engem Zusammenhang mit der eben entwickelten Eigenschaft der elementaren symmetrischen Form steht die Auswertung der Determinante

$$| \mathfrak{f}_{rs} |_{(r,s=1,\ldots,m)},$$

wo

$$\mathfrak{f}_{rs} = \frac{\partial \mathfrak{f}_r}{\partial x_s}$$

*) „Demonstratio nova altera" Werke Bd. III, pag. 31.

ist, wie dies die Theorie der „Funktionaldeterminanten“ (Kap. V § 15) zeigen wird.

Zu diesem Zweck gehen wir von der § 10 aufgestellten Identität aus:

$$P(z) = (z - x_1) \cdots (z - x_m) = \sum_{r=0}^{m} (-1)^r \mathfrak{f}_r z^{m-r}.$$

Deriviert man nach x_s, so wird

$$\frac{\partial}{\partial x_s} P(z) = \sum_{r=1}^{m} (-1)^r \mathfrak{f}_{rs} z^{m-r}. \tag{1}$$

Man hat aber auch

$$\frac{\partial}{\partial x_s} P(z) = -\prod_{h=1}^{m}{}^{(s)} (z - x_h),$$

wenn das Zeichen $\prod_{h=1}^{m}{}^{(s)}$ die Bildung des Produkts mit Ausschluß jenes Faktors bedeutet, bei dem $h = s$ sein würde. Schreibt man noch

$$P'(z) = \frac{\partial}{\partial z} P(z) = \sum_{i=1}^{m} \prod_{h=1}^{m}{}^{(i)} (z - x_h),$$

so wird, wenn man in (1) x_i für z setzt:

$$\sum_{r=1}^{m} (-1)^{r-1} \mathfrak{f}_{rs} x_i^{m-r}$$

gleich $P'(x_i)$ oder 0, je nachdem i gleich s oder von s verschieden ist, eine Bestimmung, die, wenn man nach Kronecker das Zeichen δ_{gh} mit der Bedeutung

$$\delta_{gg} = 1, \quad \delta_{gh} = 0 \qquad (g \neq h)$$

einführt, in der einheitlichen Gestalt

$$\sum_{r=1}^{m} (-1)^{r-1} \mathfrak{f}_{rs} x_i^{m-r} = \delta_{is} P'(x_i) \qquad (i, s = 1, \ldots, m) \tag{D}$$

geschrieben werden kann.

Hieraus folgt unmittelbar nach dem Multiplikationssatz der Determinanten die Relation:

$$|(-1)^{r-1} \mathfrak{f}_{rs}| \, |x_i^{m-r}| = \prod_{i=1}^{m} P'(x_i) \qquad (i, r, s = 1, 2, \ldots, m)$$

oder, da rechts $x_i - x_j$ je zweimal, aber mit entgegengesetztem Vorzeichen erscheint, auch

$$= (-1)^{\frac{m(m-1)}{2}} \prod_{r,s} (x_r - x_s)^2. \qquad (r < s)$$

Hebt man nun links in jeder Spalte der ersten Determinante $(-1)^{r-1}$ $(r = 1, \ldots, m)$, rechts entsprechend $(-1)^{\frac{m(m-1)}{2}}$, so erhält man

$$|f_{rs}|\,|x_i^{m-r}| = \prod_{r,s} (x_r - x_s)^2$$

oder mit Rücksicht auf (III) in § 11 schließlich:

$$|f_{rs}|_{(r,s=1,\ldots,m)} = |x_i^{m-j}|_{(i,j=1,\ldots,m)} = \prod_{r,s} (x_r - x_s). \qquad \begin{pmatrix} r, s = 1, \ldots, m \\ r < s \end{pmatrix}$$

§ 16. Wir beweisen nun das folgende einfache, aber vielfach nützliche Lemma aus der Theorie der Determinanten.

Wenn für die Determinanten

$$A = |a_{rs}|, \qquad B = |b_{ij}|,$$
$$(r, s = 1, \ldots, m) \qquad (i, j = 1, \ldots, m)$$

die Komposition der Spalten in der ersten Determinante mit den Zeilen in der zweiten Determinante

$$\sum_{k=1}^{m} a_{ks} b_{ik} = \delta_{is} \qquad (1)$$

ergibt, so ist auch bei Komposition der Zeilen der ersten Determinante mit den Spalten der zweiten

$$\sum_{k=1}^{m} a_{rk} b_{kj} = \delta_{rj}, \qquad (2)$$

wo das Zeichen δ_{gh} die früher festgetzte Bedeutung hat.

Die festgesetzten Gleichungen (1), der Zahl nach m^2, sind unmittelbar m Systeme von linearen Gleichungen, die einzeln für irgend einen Wert von i die m Größen b_{ik} $(k = 1, \ldots, m)$ ergeben, und zwar wird, wenn man in gewohnter Weise die den Elementen a_{rs}, b_{ij} adjungierten Unterdeterminanten mit A_{rs} und B_{ij} bezeichnet,

$$A b_{ik} = \sum_{s=1}^{m} \delta_{is} A_{ks} = A_{ki}.$$

Dann ist aber

$$A\sum_{k=1}^{m} a_{rk}b_{kj} = \sum_{k=1}^{m} a_{rk}A_{jk} = \delta_{rj}A,$$

woraus, da $AB = 1$, also A nicht null ist, in der That die unter (2) aufgeführten Relationen folgen.

Wir gehen nun von dem holoiden Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ zu dem entsprechenden orthoiden Bereiche über, was nach § 4 des ersten Kapitels gestattet ist, und erhalten in

$$|(-1)^{r-1}\mathsf{f}_{rs}| \quad \text{und} \quad \left|\frac{x_i^{m-r}}{P'(x_i)}\right| \qquad (i, r, s = 1, 2, \ldots, m)$$

zwei Determinanten, die nach der Gleichung (D) in § 15 den Bedingungen des eben erwiesenen Lemmas genügen. Man erhält also unmittelbar die folgenden von Kronecker aufgestellten Relationen

$$\sum_{k=1}^{m} \frac{(-1)^{r-1}\mathsf{f}_{rk}x_k^{m-j}}{P'(x_k)} = \delta_{rj}, \qquad \text{(E)}$$

die insbesondere für $r = 1$ die sog. Eulerschen Formeln ergeben*). Da nämlich, wie unmittelbar zu sehen,

$$\mathsf{f}_{1k} = \frac{\partial \mathsf{f}_1}{\partial x_k} = 1,$$

ist in diesem Falle:

$$\sum_{k=1}^{m} \frac{x_k^{m-j}}{P'(x_k)} = \delta_{1j}. \qquad \text{(E')}$$

Wenn wir in (E) mit x^{m-r} multiplizieren und die für $r = 1, \ldots, m$ resultierenden Gleichungen addieren, so erhält man

$$\sum_{k=1}^{m} \frac{x_k^{m-j}\sum_{r=1}^{m}(-1)^{r-1}\mathsf{f}_{rk}x^{m-r}}{P'(x_k)} = x^{m-j} \quad (j = 1, \ldots, m).$$

Hierin ist aber nach § 15

$$\sum_{r=1}^{m}(-1)^{r-1}\mathsf{f}_{rk}x^{m-r} = \prod_{h=1}^{m}{}^{(k)}(x - x_h) = P_k(x),$$

*) „Über die symmetrischen Funktionen". Mon.-Ber. Berl. Ak. 1880, pag. 948 (Werke, Bd. IV).

wenn man das Produkt der Faktoren $x - x_h$ $(h = 1, \ldots, m)$ mit Ausschluß von $x - x_k$ kurz mit $P_k(x)$ bezeichnet, also endlich

$$\sum_{k=1}^{m} \frac{x_k^{m-j} P_k(x)}{P'(x_k)} = x^{m-j} \qquad (j = 1, \ldots, m), \qquad \text{(L')}$$

eine Formel, die den Übergang zur Theorie der ganzen Funktionen, insbesondere ihre Bestimmung durch gegebene Werte im Sinne des § 2 dieses Kapitels vermitteln wird.

Die ganzen Funktionen.

§ 17. Aus der Definition

$$P(x) = \prod_{k=1}^{m} (x - x_k)$$

ergibt sich unmittelbar

$$\frac{\partial}{\partial x} P(x) = P'(x) = \sum_{k=1}^{m} P_k(x),$$

und demnach

$$P'(x_k) = P_k(x_k)$$

als von 0 verschiedene Größe. Dagegen ist

$$P_k(x_h) = 0 \qquad (h \neq k)$$

und also schließlich

$$\frac{P_k(x_h)}{P'(x_k)} = \delta_{hk}.$$

Dies führt nicht nur auf einem von den vorhergehenden Erörterungen unabhängigen Wege zu den Gleichungen (L'), sondern auch sogleich zu der in ihnen enthaltenen, aber formell allgemeineren Lagrangeschen Interpolationsformel.

Ist nämlich

$$f(x) = A_0 + A_1 x + \cdots + A_{m-1} x^{m-1}$$

eine ganze Funktion von x, die den Grad m nicht erreicht und für $x = x_k$ $(k = 1, \ldots, m)$ die Werte $f(x_k)$ annimmt, so wird

$$f(x) = \sum_{k=1}^{m} \frac{f(x_k) P_k(x)}{P'(x_k)}. \qquad \text{(L)}$$

Daß der Ausdruck rechts für $x = x_k$ wirklich immer gleich $f(x_k)$ wird, ist unmittelbar klar. Daß er mit $f(x)$ vollständig übereinstimmen muß, folgt aus dem einfachen, aber grundlegenden Satze:

Es gibt eine und nur eine ganze Funktion, die den Grad m nicht erreicht und für m verschiedene Werte von x gegebene Werte annimmt.

Man erhält nämlich durch diese Bedingungen für die Koeffizienten der ganzen Funktion die Gleichungen

$$A_0 + A_1 x_k + A_2 x_k^2 + \cdots + A_{m-1} x_k^{m-1} = f(x_k)$$
$$(k = 1, \ldots, m),$$

also ein lineares System zur Bestimmung der A_i, dessen Determinante $[x_1^{m-1}]$ nicht verschwindet und demnach eine eindeutige Bestimmung der Größen A_i liefert.

Dabei ist aber wohl zu beachten, daß, wenn auch die Größen x_k und $f(x_k)$ dem Bereiche [A] angehören, die entsprechende ganze Funktion im allgemeinen solche Koeffizienten besitzt, die sich nur in dem zugeordneten orthoiden Bereiche (A) finden. (Es ist z. B. jene ganze Funktion ersten Grades, für die $f(3) = 3$ und $f(9) = 7$ wird, $\frac{2}{3}x + 1$).

Derselbe Satz kann auch folgendermaßen gefaßt werden:

Sind $\xi_1, \xi_2, \ldots, \xi_{n+1}$ verschiedene Größen und ist $f(x)$ eine ganze Funktion, die den Grad n nicht übersteigt und deren Koeffizienten nicht sämtlich verschwinden, so können die Größen $f(\xi_1), f(\xi_2), \ldots, f(\xi_{n+1})$ nicht sämtlich verschwinden.

Im entgegengesetzten Falle wären nämlich 0 und $f(x)$ zwei verschiedene ganze Funktionen, die den Grad $n + 1$ nicht erreichen und für $n + 1$ verschiedene Werte des x gleiche Werte annehmen.

Die zuletzt gegebene Gestalt des Satzes führt unmittelbar zu folgender Verallgemeinerung:

Sei $F(x_1, x_2, \ldots, x_m)$ eine ganze Funktion der m Unbestimmten $x_1, x_2, \ldots, x_m$ von nicht höherer als der

n^{ten} Dimension, deren Koeffizienten nicht sämtlich verschwinden; seien ferner

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{i,n+1} \qquad (i = 1, \ldots, m)$$

m Reihen von je $n+1$ verschiedenen Größen; dann kann man aus ihnen wenigstens ein Wertsystem

$$\xi_{1r_1}, \xi_{2r_2}, \ldots, \xi_{mr_m} \quad (r_i = 1, \ldots, n+1)$$

bilden, so daß

$$F(\xi_{1r_1}, \xi_{2r_2}, \ldots, \xi_{mr_m})$$

nicht verschwindet.

Die allgemeine Richtigkeit des Satzes, die für $m = 1$ soeben bewiesen wurde, läßt sich leicht durch volle Induktion erhärten.

Ordnet man nämlich nach Potenzen von x_m:

$$F(x_1, x_2, \ldots, x_m) = X_0 + X_1 x_m + \cdots + X_n x_m^n,$$

so müßte im entgegengesetzten Falle jede Funktion X_i der $m-1$ Unbestimmten $x_1, \ldots, x_{m-1}$, deren Dimension wieder $\leqq n$ ist, für alle Wertesysteme

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{i,n+1} \qquad (i = 1, \ldots, m-1)$$

verschwinden, was dem für $m-1$ Unbestimmte als richtig angenommenen Satze widerspricht.

Wir geben endlich noch dem Satze die folgende, nur formell verschiedene Fassung, in der er am häufigsten zur Anwendung gelangt:

Seien $F_1, F_2, \ldots, F_k$ beliebig viele dem Bereiche [A] entstammende, von 0 verschiedene Formen der Unbestimmten $x_1, \ldots, x_m$, dann kann man immer beliebig viele einer in [A] enthaltenen unbegrenzten Größenreihe angehörige Systeme $\xi_1, \ldots, \xi_m$, unter anderem also auch beliebig viele solche aus rationalen und ganzen Zahlen bestehende Systeme bestimmen, so daß sämtliche Größen:

$$F_i(\xi_1, \xi_2, \ldots, \xi_m) \qquad (i = 1, 2, \ldots, k)$$

von Null verschieden sind.

Man hat zu diesem Zwecke nur $F = F_1 F_2 \ldots F_k$ zu bilden und, wenn die Dimension dieser Form oder ganzen

Funktion n ist, die Größen ξ_{ij} $(i = 1, \ldots, m;\ j = 1, \ldots, n+1)$ so zu wählen, daß die Reihe $\xi_{i1}, \xi_{i2}, \ldots, \xi_{i,n+1}$ nur voneinander verschiedene Größen enthält. Unter diesen findet sich jedenfalls ein den gegebenen Bedingungen genügendes Wertsystem. Hat man also aus [A] irgend eine unbegrenzte Reihe von Größen herausgehoben, wie z. B. die Reihe der rationalen und ganzen Zahlen, so kann man schon in dieser eine unbegrenzte Reihe von Wertsystemen bestimmen, die den aufgestellten Bedingungen genügen.

Lineare Transformation. Reguläre Formen.

§ 18. Die durch die Formeln

$$x_i = u_{i1}y_1 + u_{i2}y_2 + \cdots + u_{im}y_m \qquad (i = 1, 2, \ldots, m) \qquad \text{(T)}$$

bestimmte (homogene) lineare Transformation (oder Substitution) führt die Form $F(x_1, \ldots, x_m)$, indem man einfach in F für jedes x_i die rechte Seite der entsprechenden Gleichung in (T) setzt, in die transformierte Form $\overline{F}(y_1, \ldots, y_m)$ der Unbestimmten $y_1, \ldots, y_m$ über, die gelegentlich auch mit T(F) bezeichnet werden soll. Die Größen u_{ij} mögen dabei als Größen des zu Grunde liegenden Bereichs [A] angesehen werden und die Koeffizienten der Transformation genannt werden. Die Determinante

$$U = |u_{ij}| \qquad (i, j = 1, 2, \ldots, m)$$

heißt die Determinante der linearen Transformation und soll immer als von 0 verschieden vorausgesetzt werden.

Löst man die Gleichungen (T) nach den $y_1, \ldots, y_m$ auf, so erhält man die durch die Formeln:

$$y_j = \frac{U_{1j}x_1 + U_{2j}x_2 + \cdots + U_{mj}x_m}{U} \qquad (\mathrm{T}^{(-1)})$$

bestimmte reziproke lineare Transformation, wo U_{ij} in gewohnter Weise die dem Elemente u_{ij} adjungierte Unterdeterminante bedeutet. (Dabei sind wir wohl im allgemeinen — wegen des Nenners U — in den orthoiden Bereich (A)

übergegangen; aber nur aus Bequemlichkeitsgründen, um die mit der Vermeidung des Nenners verbundene weitläufige Schreibweise zu kürzen.) Diese reziproke Transformation ($T^{(-1)}$) führt, wie unmittelbar ersichtlich, $\overline{F}(y_1, \ldots, y_m)$ wieder in $F(x_1, \ldots, x_m)$ über.

Die ursprüngliche Form $F(x_1, \ldots, x_m)$ und die transformierte Form $\overline{F}(y_1, \ldots, y_m)$ sind von gleicher Dimension. Wären nämlich die Dimensionen von F und $\overline{F}$ z. B. n und $\overline{n}$, so kann, wie der Ausdruck für $\overline{F}$ unmittelbar zeigt, die Dimension durch die Transformation keinesfalls erhöht werden; es ist also jedenfalls $\overline{n} \leqq n$; da aber im Bereiche (A) auch $\overline{F}$ als ursprüngliche und F als transformierte Form angesehen werden kann, muß auch $n \leqq \overline{n}$ sein; und hieraus folgt eben $n = \overline{n}$.

Die Anweisung zur Ausführung der linearen Transformation zeigt ferner sogleich, daß die Koeffizienten der transformierten Form dem Bereiche [A] entstammende Formen der Transformationskoeffizienten sind, deren Dimension die Dimension der ursprünglichen Form nicht übersteigt.

Wenn man auf die durch Anwendung von (T) aus $F(x_1, \ldots, x_m)$ entstandene Form $\overline{F}(y_1, \ldots, y_m)$ wieder eine lineare Transformation anwendet, die durch

$$y_j = v_{j1} z_1 + v_{j2} z_2 + \cdots + v_{jm} z_m \qquad (T')$$

gegeben sei, so entsteht eine dritte Form $\overline{\overline{F}}(z_1, \ldots, z_m)$, die man aber auch direkt aus F durch die lineare Transformation

$$x_i = w_{i1} z_1 + \cdots + w_{ij} z_j + \cdots + w_{im} z_m \qquad (T'')$$

erhalten kann, wenn

$$w_{ij} = u_{i1} v_{1j} + u_{i2} v_{2j} + \cdots + u_{im} v_{mj}$$

gesetzt wird, denn zur Bildung von $\overline{\overline{F}}$ hat man in F für x_i die rechten Seiten der Gleichungen (T), und hier wieder für y_j die rechten Seiten der Gleichungen (T') einzusetzen.

Die Determinante der Transformation T'' ist dabei nach

dem Bildungsgesetze der Größen w_{ij} und dem Multiplikationssatze der Determinanten:

$$|w_{ij}| = |u_{ij}|\,|v_{ij}|.$$

Die Folge zweier (oder auch mehrerer) linearer Transformationen ist also wieder eine lineare Transformation, und die Determinante der resultierenden Transformation das Produkt der Determinanten der einzelnen Transformationen.

§ 19. Die Form $F(x_1, \ldots, x_m)$, deren Dimension gleich n sei, heißt regulär in Bezug auf x_i, wenn das Glied mit x_i^n einen von 0 verschiedenen Koeffizienten besitzt; sie heißt regulär — ohne weiteren Zusatz —, wenn sie in Bezug auf jede Unbestimmte regulär ist.

Wir beweisen dann leicht den folgenden wichtigen Satz:

Seien $F_1, F_2, \ldots, F_k$ beliebig viele Formen der Unbestimmten $x_1, \ldots, x_m$; dann gibt es beliebig viele lineare Transformationen, deren Koeffizienten rationale und ganze Zahlen sind und deren Determinante gleich eins ist, die sämtliche gegebenen Formen in reguläre Formen überführen,

Es sei — ausführlich geschrieben —

$$F_i = \sum_{(g)} A_g^{(i)} x_1^{g_1} x_2^{g_2} \ldots x_m^{g_m} \quad (i = 1, \ldots, k).$$

Die Anwendung der folgenden speziellen linearen Transformation

$$x_1 = y_1, \quad x_j = u_{j1} y_1 + y_j \quad (j = 2, \ldots, m),$$

wo die passende Bestimmung der Größen u_{j1} noch vorbehalten bleibt, deren Determinante aber von diesen unabhängig den Wert 1 besitzt, ergibt

$$\overline{F}_i = \sum_{(g)} A_g^{(i)} y_1^{g_1} (u_{21} y_1 + y_2)^{g_2} \ldots (u_{m1} y_1 + y_m)^{g_m}$$

und hier als Koeffizienten für y_1^n

$$\sum A_g^{(i)} u_{21}^{g_2} u_{31}^{g_3} \ldots u_{m1}^{g_m}, \tag{I}$$

wo die Summation sich auf alle jene Glieder erstreckt, für die

$g_1 + g_2 + \cdots + g_m = n$ war; zugleich sind die Koeffizienten der Glieder mit y_j^n $(j \geqq 2)$ dieselben, wie die Koeffizienten der Glieder mit x_j^n in F_i. Man kann also in der Tat nach dem Satze am Schlusse des vorhergehenden Paragraphen solche rationale ganze Zahlen für $u_{21}, \ldots, u_{m1}$ wählen, daß sämtliche Ausdrücke in (I) für $i = 1, 2, \ldots, k$ von 0 verschiedene Werte annehmen, also die Formen $\bar{F}_1, \ldots, \bar{F}_k$ in Bezug auf y_1 regulär werden.

Damit ist aber der wesentliche Teil des Beweises erledigt. Wenn es nämlich in dieser Weise gelungen ist, die gegebenen Formen in solche zu transformieren, die in Bezug auf eine bestimmte Anzahl der Unbestimmten, z. B. l, regulär ist, so wird eine neue Transformation, welche wieder die angegebene spezielle Gestalt besitzt, transformierte Formen liefern, die in Bezug auf eine gewisse $l + 1^{\text{te}}$ Unbestimmte regulär sind, während die Koeffizienten der Glieder, die die n^{ten} Potenzen jener l Unbestimmten enthalten, sich überhaupt nicht ändern, so daß die neuen Formen auch für diese, im ganzen also in Bezug auf $l + 1$ Unbestimmte regulär sind.

Man gelangt also schließlich zu Formen, die in Bezug auf alle Unbestimmte regulär sind, und zwar mit Hilfe einer linearen Transformation, die als Folge jener speziellen Transformationen leicht darstellbar ist. Man erkennt nun unmittelbar, daß mit den Größen u_{ij} auch die Koeffizienten dieser resultierenden Transformation rationale und ganze Zahlen sind und daß ihre Determinante, als Produkt von Determinanten, deren jede gleich eins ist, wieder gleich eins sein muß.

Die „allgemeine“ (homogene) lineare Transformation wird gleichfalls durch die Gleichungen

$$x_i = u_{i1} y_1 + u_{i2} y_2 + \cdots + u_{im} y_m \qquad (i = 1, \ldots, m) \qquad \text{(T)}$$

definiert, wo aber nun die Koeffizienten der Transformation, u_{ij}, als neue Unbestimmte zu betrachten sind. Die Koeffizienten der transformierten Form sind dann dem Bereiche [A] entstammende Formen der Unbestimmten u_{ij}, und jede Form wird nach Ausübung der allgemeinen linearen Transformation re-

gulär; denn die fraglichen Koeffizienten sind auch dann nicht Null, wenn man statt der u_{ij} die früher bestimmten speziellen Werte einführt; sie werden also im „allgemeinen" Falle von 0 verschiedene Formen sein. Wäre nämlich die durch allgemeine Transformation erlangte Form nicht regulär, so könnte dies für gewisse Werte der u nur dadurch stattfinden, daß die Glieder n^{ter} Dimension sämtlich verschwinden. Dies ist aber nicht der Fall, denn die zu Hilfe genommene spezielle Transformation läßt die Dimension der Form ungeändert.

Drittes Kapitel.

Die Teilbarkeit der Formen.

Das gewöhnliche Divisionsverfahren.

§ 1. Der Bereich [A], von dem wir wieder ausgehen, ist in Bezug auf die in ihm herrschenden Teilbarkeitsverhältnisse nur dann als wohldefiniert zu betrachten, wenn eine Methode vorliegt, die es gestattet, „die vollständige Diskussion der Gleichung ersten Grades“ $\beta x = \alpha$, $(\beta \neq 0)$ in einer endlichen Anzahl von Schritten zu erledigen, d. h. in der angegebenen Weise darüber zu entscheiden, ob α durch β teilbar ist und, wenn dies der Fall ist, den Wert $x = \beta'$ (den zu β komplementären Teiler von α) liefert. Insbesondere ist dies nach den Elementen der Arithmetik für den Bereich [1] der Fall; ebenso für jeden orthoiden Bereich, da die gesuchte Größe unmittelbar in der Form $\frac{\alpha}{\beta}$ gegeben ist.

Unsere erste Aufgabe ist es, zu zeigen, daß mit [A] immer auch $[A, x_1, x_2, \ldots, x_m]$ ein in dem angegebenen Sinne wohldefinierter Bereich ist. Zu diesem Zwecke muß bloß das in den Elementen gelehrte gewöhnliche Divisionsverfahren genau präcisiert werden. Da dem Wesen der Sache nach wieder die vollständige Induktion zur Anwendung gelangt, mag noch besonders betont werden, daß der Bereich [A] schon beliebig viele Unbestimmte enthalten kann. Geht man dann durch Hinzufügung der Unbestimmten x zum Bereiche $[A, x]$ über, so ist der Inhalt jenes gewöhnlichen Divisionsverfahrens in folgendem Satze enthalten:

Seien (für $m \geqq n$, $A_0 \neq 0$, $B_0 \neq 0$)

$$F = A_0 x^m + A_1 x^{m-1} + \cdots + A_m$$
$$G = B_0 x^n + B_1 x^{n-1} + \cdots + B_n$$

zwei Formen des Bereichs [A, x], also A_i, B_j Größen aus [A], so gibt es immer eine und nur eine Form Q im Bereiche [A, x] von der Beschaffenheit, daß

$$R = B_0^{m-n+1} F - GQ$$

eine Form vom höchstens $n - 1^{\text{ten}}$ Grade in x wird.

Dabei nennt man Q resp. R den Quotienten, resp. den Rest, der bei der „Division von $B_0^{m-n+1} F$ durch G“ auftritt.

Der aufgestellten Bedingung gemäß kann Q den Grad $m - n$ nicht übersteigen, sonst wäre R vom Grade $m + 1 \geqq n + 1$, Q kann aber auch nicht von niedrigerem, als dem $m - n^{\text{ten}}$ Grade sein, sonst würde GQ den Grad m nicht erreichen, also wäre R vom m^{ten} Grade. Es hat also die Form Q, wenn sie überhaupt existiert, jedenfalls die Gestalt

$$Q = Q_0 x^{m-n} + Q_1 x^{m-n-1} + \cdots + Q_{m-n},$$

wo $Q_0 \neq 0$. Da nun in R die Koeffizienten von $x^n, x^{n+1}, \ldots, x^m$ gleich 0 sein müssen, so erhält man zur Bestimmung der Größen Q_i das System linearer Gleichungen:

$$B_0^{m-n+1} A_i = B_i Q_0 + B_{i-1} Q_1 + \cdots + B_0 Q_i \qquad \text{(I)}$$
$$(i = 0, 1, \ldots, m - n),$$

welches in der Tat die Größen Q_i eindeutig als dem Bereiche [A] angehörige Größen bestimmt; denn die aus den Koeffizienten der Unbekannten gebildete Determinante B_0^{m-n+1} ist von Null verschieden, und man hat zur Bestimmung von Q_i

$$B_0^{m-n+1} Q_i = D_i, \qquad \text{(Ia)}$$

wo die rechts stehende Größe D_i sich unmittelbar als durch B_0^{m-n+1} teilbar erweist; denn sie ist als Determinante dargestellt, in welcher sämtliche Elemente der $i + 1^{\text{ten}}$ Spalte durch B_0^{m-n+1} teilbar sind.

Nach dieser Bestimmung der Größen Q_i ergeben sich die Koeffizienten der Form

$$R = R_0 x^{n-1} + R_1 x^{n-2} + \cdots + R_{n-1}$$

unmittelbar:

$$R_j = B_0^{m-n+1} A_{m-n+j+1} - B_{j+1} Q_{m-n} - B_{j+2} Q_{m-n-1} - \cdots \qquad \text{(II)}$$
$$(j = 0, 1, \ldots, n-1),$$

wo die Werte der Q_i aus (Ia) einzusetzen sind.

Das Kriterium der Teilbarkeit im Formenbereiche.

§ 2. Die notwendigen und hinreichenden Bedingungen für die Teilbarkeit von

$$F = A_0 x^m + \cdots + A_m \qquad (A_0 \neq 0)$$

durch

$$G = B_0 x^n + \cdots + B_n \qquad (B_0 \neq 0)$$

sind die folgenden: Es muß $m \geqq n$ sein, es müssen ferner die (im vorhergehenden Paragraphen definierten) Größen R_j $(j = 0, \ldots, n-1)$ verschwinden, und schließlich die ebendort definierten Größen Q_i $(i = 0, \ldots, m-n)$ durch B_0^{m-n+1} teilbar sein.

Soll nämlich

$$F = GH$$

sein, wo wieder H eine Form des Bereichs $[\mathsf{A}, x]$ ist, so muß in der Tat $m \geqq n$ sein, und die aus dem Divisionsverfahren herrührende Relation

$$B_0^{m-n+1} F = GQ + R$$

mit der aus der Tatsache der Teilbarkeit stammenden Relation

$$B_0^{m-n+1} F = G B_0^{m-n+1} H$$

derart übereinstimmen, daß

$$R = 0, \quad Q = B_0^{m-n+1} H$$

wird. Es muß also in der Tat $R_j = 0$ sein und, wenn man ausführlich

$$H = H_0 x^{m-n} + \cdots + H_{m-n}$$

schreibt, auch

$$Q_i = B_0^{m-n+1} H_i$$

werden.

Damit ist die Frage der Teilbarkeit aus dem Bereiche $[\mathsf{A}, x]$ in den Bereich $[\mathsf{A}]$ übertragen, also auch, wenn die vor-

gelegten Formen dem Bereiche $[A, x_1, \ldots, x_m]$ angehören, die Teilbarkeit der einen durch die andere auf die entsprechende Untersuchung in $[A, x_1, \ldots, x_{m-1}]$, und so fort, schließlich also in $[A]$ zurückgeführt.

§ 3. Die Methode der linearen Transformation gestattet die Frage der Teilbarkeit von F durch G unmittelbar aus dem Bereiche $[A, x_1, \ldots, x_m]$ in den Bereich $[A]$ zu überführen. Dies zeigt die folgende einfache Betrachtung.

Sei T eine lineare Transformation, deren Koeffizienten rationale und ganze Zahlen sind, und deren Determinante gleich Eins ist, so folgt (Kap. II § 18. 19) aus

$$F = GH$$

auch

$$\overline{F} = \overline{G}\,\overline{H}$$

und umgekehrt. Die Frage der Teilbarkeit kann also ebenso an den transformierten Formen $\overline{F}$ und $\overline{G}$ entschieden werden. An der angeführten Stelle wurde nun bewiesen, daß die rationalen und ganzen Koeffizienten jener linearen Transformation auch so gewählt werden können, daß die Form $\overline{G}$ regulär wird, d. h. daß in ihrem höchsten Gliede $\overline{B}_0 y^n$, da die Dimension jetzt mit dem Grade in y_1 übereinstimmt, der Koeffizient $\overline{B}_0$ eine von 0 verschiedene Größe des Bereichs $[A]$ wird.

Die Teilbarkeit von Q durch $\overline{B}_0{}^{m-n+1}$ erfordert nun einfach die Teilbarkeit sämtlicher Koeffizienten, wird also in der Tat im Bereiche $[A]$ entschieden.

Aus der Definition der regulären Formen folgt unmittelbar, daß das Produkt zweier Formen G und H nur dann regulär in Bezug auf x_1 sein kann, wenn die Formen G und H selbst regulär in Bezug auf x_1 sind.

Hat man

$$G = G_0 x_1{}^n + \cdots + G_n,$$
$$H = H_0 x_1{}^p + \cdots + H_p,$$

also

$$GH = G_0 H_0 x_1{}^{n+p} + \cdots + G_n H_p,$$

so ist diese Form nur dann regulär, wenn ihre Dimension gleich dem Grade in x_1, d. h. gleich $n+p$ ist; dann muß aber $G_0 H_0$, also auch G_0 und H_0 dem Bereiche [A] angehören und von 0 verschieden sein; andererseits haben G und H die Dimension n resp. p; das erste Glied zeigt, daß G und H mindestens diese Dimension erreichen; würde aber auch nur eine der beiden Formen diese Dimension überschreiten, so wäre ihr Produkt von höherer als der $n+p^{\text{ten}}$ Dimension. Es sind also in der Tat G und H reguläre Formen.

Die folgende Gestalt des soeben bewiesenen Satzes zeigt seine Stelle in dieser elementaren Untersuchung der Teilbarkeit:

Eine in Bezug auf gewisse Unbestimmte reguläre Form kann nur solche Formen als Teiler besitzen, die in Bezug auf diese Unbestimmte selbst regulär sind.

Der Dedekindsche Hilfssatz.

§ 4. Es seien

$$a_0, a_1, \ldots, a_m$$

$m+1$ Größen, die irgend einem holoiden Bereiche angehören; (oder auch allgemeiner irgend einem Bereiche, dessen Größen ein gewöhnliches Additions- und Multiplikationsgesetz besitzen). Man bilde sodann sämtliche Potenzprodukte der Größen $a_0, \ldots, a_m$ von der Dimension $n+1$, wo n eine nicht negative rationale und ganze Zahl bedeutet:

$$P_r = a_0^{r_0} a_1^{r_1} \ldots a_m^{r_m},$$

wo also die r wieder nicht negative rationale und ganze Zahlen sind, die der Relation:

$$r_0 + r_1 + \cdots + r_m = n + 1$$

genügen. Die Anzahl der Potenzprodukte P_r ist dabei nichts anderes als die Anzahl der möglichen Glieder in einer homogenen Form $n+1^{\text{ter}}$ Dimension von $m+1$ Unbestimmten, also nach Kap. 2 § 8 $\binom{m+n+1}{n+1}$.

Andererseits bilde man aus den Größen $a_0, \ldots, a_m$ das folgende aus $m+n+1$ Zeilen und $n+1$ Spalten bestehende

Schema, die wegen der aus ihm zu erzeugenden Determinanten sogenannte (Determinanten-)Matrix:

$$\|a_{i-j}\| \quad (i = 1, \ldots, m+n+1;\ j = 1, \ldots, n+1), \qquad \text{(M)}$$

wo noch a_r gleich Null zu setzen ist, wenn r negativ oder größer als m ist. Das Gesetz dieser Matrix, wie es aus der gegebenen Bestimmung abgelesen werden kann, ist in ausführlicherer Gestalt das folgende: Die j^{te} Spalte enthält in der Reihenfolge der Zeilen folgende Größen: $j-1$-mal die Null, dann $a_0, a_1, \ldots, a_m$ und endlich wieder $n-j+1$-mal die Null. Zur leichteren Übersicht sei noch ausnahmsweise die Matrix auch ausführlich hingeschrieben:

$$\left\| \begin{array}{ccccc} a_0 & & & & \\ a_1 & a_0 & & & \\ . & a_1 & . & & \\ . & . & . & . & \\ . & . & . & . & a_0 \\ a_m & . & . & . & a_1 \\ & a_m & . & . & . \\ & & . & . & . \\ & & & . & . \\ & & & & a_m \end{array} \right\|, \qquad \text{(M)}$$

wo an die leeren (auch nicht punktierten) Stellen die Null zu setzen ist. Diese Matrix definiert unmittelbar die Determinanten

$$D_s = |a_{i-j}|, \qquad \left(\begin{array}{c} i = s_0, s_1, \ldots, s_m;\ j = 1, \ldots, n+1 \\ s_h = 1, 2, \ldots, m+n+1 \end{array}\right),$$

deren Anzahl, wenn wir nur jene als wesentlich verschiedene zulassen, die sich nicht bloß in der Reihenfolge der aus der Matrix entnommenen Zeilen unterscheiden, wieder gleich $\binom{m+n+1}{n+1}$ ist, da ja aus $m+n+1$ Zeilen deren $n+1$ zu wählen sind. Um die Determinanten vollständig, d. h. auch in Bezug auf das Vorzeichen zu fixieren, kann man

$$s_0 < s_1 < \cdots < s_n$$

als weitere Bedingung einführen.

Schreibt man nun die Größen P_r und D_s in irgend einer Reihenfolge

$$P_\varrho, \quad D_\sigma \qquad \left(\varrho, \sigma = 1, 2, \ldots, \binom{m+n+1}{n+1}\right),$$

so gilt der Satz*):

Jede Größe P_ϱ ist eine rationale und ganze homogene lineare Form der Größen D_σ; d. h. man hat:

$$P_\varrho = \sum_{\sigma=1}^{\nu} k_{\varrho\sigma} D_\sigma, \qquad \left(\nu = \binom{m+n+1}{n+1}\right),$$

wo die Koeffizienten $k_{\varrho\sigma}$ rationale und ganze Zahlen sind.

Der umgekehrte Satz, nämlich die entsprechende Darstellung der D_σ durch die P_ϱ, ist selbstverständlich, da die Definition der Determinante eben diese Darstellung ergibt.

Um den ausgesprochenen Satz zu erweisen und jene Darstellung der Größen P_ϱ auch wirklich zu erhalten, benutzen wir die vollständige Induktion.

Wir setzen die Methode der Darstellung als gegeben voraus, wenn $m+n$ kleiner als eine bestimmte Zahl N, und entwickeln sie dann für den Fall $m+n=N$. Dies genügt; denn für $m+n=0$ ist die Richtigkeit des Satzes unmittelbar einzusehen. Dann muß $m=0$ und $n=0$ sein, also gibt es nur eine Größe a_0; die Reihe der P_ϱ reduziert sich auf die eine Größe a_0, und auch die Reihe der Größen D_σ besteht nur aus der einen Größe a_0; denn jene Matrix hat nur eine Zeile und eine Spalte, besteht also gleichfalls nur aus dem einen Elemente a_0.

Für den allgemeinen Beweis unterscheiden wir zwei Fälle,

---

*) R. Dedekind „Über einen arithmetischen Satz von Gauß". Mitteilungen der deutschen mathematischen Gesellschaft in Prag. 1892. p. 1.

Dieser Satz und der später in § 5 behandelte, die hier als elementare Identitäten erscheinen, werden von Dedekind mit Hilfe scharfsinniger, aber komplizierter Betrachtungen abgeleitet, die der von ihm geschaffenen „Theorie der Moduln" angehören.

je nachdem die zu berechnende Größe P den Faktor a_0 enthält oder nicht. Im ersten Falle kann

$$P = a_0 P'$$

geschrieben werden. Dann ist P' irgend ein Potenzprodukt der Größen $a_0, \ldots, a_m$ von der Dimension $n = (n-1) + 1$, also nach dem als richtig angenommenen Satze als rationale und ganze homogene lineare Form gewisser Determinanten D' darstellbar, die aus einer leicht zu charakterisierenden Matrix (M′) erzeugt werden. Die zur Verwendung gelangende Größenreihe ist dieselbe wie früher: $a_0, a_1, \ldots, a_m$, aber an Stelle von n ist $n-1$ getreten. (M′) entsteht aus (M) durch Weglassung der ersten Zeile und Spalte. Aus jeder Determinante D' erhält man demnach, wenn man ihr als erste Zeile die Elemente Null und dann in der ersten Spalte zuerst a_0 und dann jene Elemente vorsetzt, die in der ersten Spalte von (M) in derselben Zeile erscheinen, eine Determinante D, deren Wert ihrer Entstehung nach $a_0 D'$ ist. War nun, wie angenommen, P' eine rationale und ganze homogene lineare Form der D', so ist $a_0 P' = P$ dieselbe Form der $a_0 D'$ oder D.

Im zweiten Falle, wenn P die Größe a_0 überhaupt nicht enthält, ist P ein Potenzprodukt der $m = (m-1) + 1$ Größen $a_1, \ldots, a_m$, dessen Dimension ungeändert gleich $n+1$ bleibt, also nach dem als richtig angenommenen Satze als rationale und ganze homogene lineare Form gewisser Determinanten D'' darstellbar, die aus einer leicht zu charakterisierenden Matrix (M″) erzeugt werden. Die zur Verwendung gelangende Größenreihe ist: $a_1, \ldots, a_m$, wo also a_0 wegbleibt. (M″) entsteht aus (M), wenn man die erste Zeile wegläßt und in den übrigen Null an die Stelle von a_0 setzt. Setzt man also in D'' an jenen Stellen, wo früher a_0 stand, wieder a_0 an die Stelle von 0, so entsteht eine entsprechende Determinante D, und $D'' - D$ ist eine rationale und ganze homogene lineare Form solcher Potenzprodukte P, die den Faktor a_0 enthalten, und nach dem früher bewiesenen Teilsatze eine ebensolche Form von Determinanten D. Dasselbe ist mithin für D'' und endlich auch für P

der Fall, womit der angegebene Satz endlich auch allgemein bewiesen ist.

Der Kroneckersche Fundamentalsatz.

§ 5. Um den vorzutragenden Satz*) zuerst in einem speziellen, aber grundlegenden Falle darzulegen, seien im genauen Anschluß an die im vorhergehenden Paragraph benutzten Bezeichnungen

$$f(x) = a_0 x^m + \cdots + a_m$$
$$g(x) = b_0 x^n + \cdots + b_n$$

zwei Formen von x, deren Koeffizienten dem holoiden Bereiche [A] angehören**), und deren Produkt, abermals nach fallenden Potenzen von x geordnet,

$$f(x)\,g(x) = c_0 x^{m+n} + \cdots + c_{m+n}.$$

*) Kronecker „Zur Theorie der Formen höherer Stufen". Mon.-Ber. Berl. Akad. 1883. pag. 957 (Werke, Bd. II pag. 417).

Der Satz wurde von Kronecker erst nach Publikation der „Festschrift" gefunden und in dieser selbst nicht verwendet. Er blieb, wie es scheint, ganz unbeachtet, bis Dedekind an der früher erwähnten Stelle den in § 5 behandelten speziellen Fall selbständig neu entdeckte und dann insbesondere Hurwitz seine Wichtigkeit erwies. („Über die Theorie der Ideale". Nachr. d. Kgl. Ges. d. Wiss. zu Göttingen 1894. pag. 290).

Dies ist um so merkwürdiger, als schon Molk in seiner Abhandlung: „Sur une notion générale, qui comprend celle de la divisibilité etc." (Acta mathematica, Bd. VI pag. 71) den Satz gebraucht, und Kronecker selbst in den einleitenden Worten jener Note auf dessen Wichtigkeit mit folgenden Worten hinweist: „Das Streben nach Erforschung der einfachsten Grundlagen der Theorie der Formen hat mich schon vor langer Zeit auf eine Frage geführt, die dem Anscheine nach ganz elementar ist, und die ich dennoch nicht früher zu erledigen vermochte."

Die absolut elementare Darstellung und Beweisführung des Satzes, die hier gegeben wird, gestattet es, ihn als Ausgangspunkt der Theorie zu benutzen, wodurch das ganze System überraschend einfach und durchsichtig wird.

**) Es sei noch einmal erwähnt, daß hier wie auch im folgenden Paragraphen von den Eigenschaften des Bereichs [A] nur die benutzt wird, daß dessen Größen ein gewöhnliches Additions- und Multiplikationsgesetz besitzen.

Es bestehen dann zwischen den Koeffizienten a, b, c die folgenden Relationen:

$$a_t b_0 + a_{t-1} b_1 + \cdots + a_{t-n} b_n = c_t \qquad (t = 0, 1, \ldots, m+n),$$

wo wieder a_r gleich Null zu setzen ist, wenn r negativ oder größer als m wird.

Wählt man aus diesen Gleichungen diejenigen aus, in denen

$$t = s_0, s_1, \ldots, s_n$$

ist, so folgt aus ihnen, wenn man $b_0, \ldots, b_n$ als Unbekannte ansieht, für irgend ein b_j:

$$D_s b_j = \sum_{t=0}^{m+n} Q_{jt}^{(s)} c_t,$$

wo D_s genau die im vorhergehenden Paragraph auftretende Determinante ist, und die Q_{jt}, als erste Unterdeterminanten von D_s, rationale und ganze homogene Formen der Größen $a_0, \ldots, a_m$ von der Dimension n sind.

Ist nun a_i wieder irgend eine der Größen $a_0, \ldots, a_m$, so wird weiter

$$D_s a_i b_j = \sum_{t=0}^{m+n} Q_{jt}^{(s)} a_i c_t$$

und die $a_i Q_{jt}$ sind rationale und ganze homogene Formen der $a_0, \ldots, a_m$ von der Dimension $n+1$. Da nun jedes Potenzprodukt der $a_0, \ldots, a_m$ von der Dimension $n+1$ eine rationale und ganze homogene lineare Form der Determinanten

$$D_\sigma \qquad \left(\sigma = 1, \ldots, \nu;\ \nu = \binom{m+n+1}{n+1}\right)$$

ist, erhält man schließlich, wenn man in dem soeben erhaltenen Ausdruck für jedes Glied von $a_i Q_{jt}$ diese Formen einsetzt und die dasselbe D_σ enthaltenden Glieder vereinigt, für irgend ein Koeffizientenprodukt $a_i b_j$ die Identitäten

$$D_s a_i b_j = \sum_{\sigma=1}^{\nu} L_{ij\sigma}^{(s)} D_\sigma, \tag{1}$$

wo die $L_{ij\sigma}^{(s)}$ rationale und ganze homogene lineare Formen der Größen $c_0, \ldots, c_{m+n}$ sind und für D_s irgend

eine Determinante der Reihe D_σ gesetzt werden kann, wobei sich die Formen $L_{ij\sigma}^{(s)}$ oder, genauer, die in ihnen als Koeffizienten auftretenden rationalen und ganzen Zahlen mit s ändern.

§ 6. Das so erhaltene Resultat ist nichts anderes als der Kroneckersche Fundamentalsatz für den einfachsten Fall zweier Formen mit einer Unbestimmten. Es wird aber für die Klarheit der weiteren Darstellung vorteilhafter sein, wenn wir zuerst den Satz in seiner allgemeinsten Gestalt aussprechen:

Es seien:

$$F_j = \sum A_g^{(j)} x_1^{g_1} \dots x_m^{g_m} \qquad (j = 1, 2, \dots, k)$$

k von Null verschiedene Formen der Unbestimmten $x_1, \dots, x_m$ (mit dem holoiden Bereiche [A] angehörigen Koeffizienten) und ihr Produkt:

$$F = F_1 \dots F_k = \sum C_g x_1^{g_1} \dots x_m^{g_m};$$

es sei ferner

$$P_i = A_{i_1}^{(1)} A_{i_2}^{(2)} \dots A_{i_k}^{(k)}$$

das Produkt von k je einer Form entnommenen Koeffizienten von $F_1, \dots, F_k$.

Dann gibt es immer eine Reihe von Größen $H_1, H_2, \dots, H_\nu$, die von Null verschiedene rationale und ganze homogene Formen der $A^{(1)}, \dots, A^{(k-1)}$ sind, und ferner eine Reihe von Größen $L_{i\sigma}^{(s)}$, die rationale und ganze homogene lineare Formen der Größen C_g sind, so daß

$$H_s P_i = \sum_{\sigma=1}^{\nu} L_{i\sigma}^{(s)} H_\sigma \qquad (s = 1, \dots, \nu) \qquad \text{(K)}$$

wird.

Für zwei Formen einer Unbestimmten ist dies genau der soeben erwiesene Satz, und die Größen H sind nichts anderes als jene Determinanten D_σ, unter denen a_0^{n+1} von Null verschieden ist, während die eventuell verschwindenden D bei der definitiven Formulierung des Satzes einfach weggelassen werden können.

Wir haben nun für den allgemeinen Fall das Bildungsgesetz jener Größen H_σ und $L_{i\sigma}^{(s)}$ aufzustellen, die den Relationen (K) genügen. Dabei kann man vor allem das ganze Problem auf den Fall reduzieren, wo die Formen nur eine Unbestimmte enthalten.

Setzt man nämlich gemäß den in Kap. II § 3 und 4 gegebenen Erörterungen

$$g = g_1 t^{m-1} + g_2 t^{m-2} + \cdots + g_m$$

und dann x^g an die Stelle von $x_1^{g_1} \ldots x_m^{g_m}$, so erhält man aus den Formen $F_1, \ldots, F_k$ und F

$$f_j = \sum A_g^{(j)} x^g$$

$$f = f_1 \cdots f_k = \sum C_g x^g,$$

wo die C_g genau auf dieselbe Weise aus den $A_g^{(j)}$ herzuleiten sind, wie früher. Gelingt es also für diese Formen, das Bildungsgesetz entsprechender Größen H_σ und $L_{i\sigma}^{(s)}$ zu ermitteln, so gilt es auch für die Formen F_j.

Dieses endgültige Bildungsgesetz ergibt sich durch vollständige Induktion.

Wir nehmen an, daß ein solches Bildungsgesetz für weniger als k Formen bekannt sei und bestimmen es dann auch für k Formen. Da für zwei Formen das Problem in der Tat schon erledigt ist, wird es auf diesem Wege auch allgemein, d. h. für ein beliebig gegebenes k gelöst.

Beschränkt man sich zuerst auf die $k-1$ Formen $f_1, \ldots, f_{k-1}$, so möge deren Produkt mit

$$\bar{f} = f_1 \cdots f_{k-1} = \sum \bar{C}_g x^g$$

bezeichnet werden. Wird entsprechend

$$\bar{P}_i = A_{i_1}^{(1)} \ldots A_{i_{k-1}}^{(k-1)}$$

gesetzt, so gibt es der Annahme nach eine Reihe von Größen $\bar{H}_1, \ldots \bar{H}_{\bar{\tau}}$, die von Null verschiedene, rationale und ganze homogene Formen der $A^{(1)}, \ldots, A^{(k-2)}$ sind, und ferner eine Reihe von Größen $\bar{L}_{i\sigma'}^{(u)}$, die rationale und ganze homogene lineare Formen der Größen $\bar{C}_g$ sind, so daß

$$\bar{H}_u \bar{P}_i = \sum_{\sigma'=1}^{\bar{\nu}} \bar{L}_{i\sigma'}^{(u)} \bar{H}_{\sigma'} \qquad (u = 1, \ldots, \bar{\nu}) \qquad (1)$$

wird. Wendet man nun den Fundamentalsatz auf den gleichfalls schon erwiesenen Fall der zwei Formen $\bar{f}$ und f_k an, deren Produkt

$$\bar{f} f_k = f = \sum C_g x^g$$

ist, so gibt es eine Reihe von Größen $h_1, \ldots, h_{\nu'}$, die von Null verschiedene, rationale und ganze homogene Formen der Größen $\bar{C}_g$, also auch der Größen $A^{(1)}, \ldots, A^{(k-1)}$ sind, und ferner eine Reihe von Größen $l_{g i_k \tau}^{(t)}$, die rationale und ganze homogene lineare Formen der Größen C_g sind, so daß

$$h_t \bar{C}_g A_{i_k}^{(k)} = \sum_{\tau=1}^{\nu} l_{g i_k \tau}^{(t)} h_\tau \qquad (t = 1, \ldots, \nu') \qquad (2)$$

wird. Multipliziert man nun (1) mit $h_t A_{i_k}^{(k)}$, so kann diese Multiplikation rechts innerhalb der Formen $\bar{L}_{i\sigma'}^{(u)}$ ausgeführt werden, wobei man durchweg Glieder von der Form (2) mit rationalen und ganzen Koeffizienten erhält. Vereinigt man jene Glieder, die dasselbe Produkt $\bar{H}_{\sigma'} h_\tau$ enthalten, so sind die Koeffizienten abermals rationale nnd ganze, homogene lineare Formen der Größen C_g, die mit $L_{i\sigma'\tau}^{(u,t)}$ bezeichnet werden können, und man hat:

$$\bar{H}_u h_t P_i = \sum_{\sigma=1}^{\bar{\nu}} \sum_{\tau=1}^{\nu'} L_{i\sigma'\tau}^{(u,t)} \bar{H}_{\sigma'} h_\tau \qquad (u = 1, \ldots, \bar{\nu};\ t = 1, \ldots, \nu').$$

Bezeichnet man schließlich die $\nu = \nu'\bar{\nu}$ Größen $\bar{H}_u h_t$ in irgend einer Reihenfolge mit $H_1, \ldots, H_s, \ldots, H_\nu$ und schreibt für $L_{i\sigma'\tau}^{(u,t)}$ einfacher $L_{i\sigma}^{(s)}$, so resultiert unmittelbar der zu beweisende Satz; denn die Größen $\bar{H}_u$, h_t und also auch ihre Produkte H_s sind sämtlich von Null verschieden.

§ 7. Bei Benutzung des schon früher gebrauchten Zeichens $\delta_{ii} = 1$, $\delta_{ij} = 0$ $(i \neq j)$ können die durch den Fundamentalsatz gegebenen Relationen (K) auf folgende Gestalt gebracht werden:

$$\sum_{\sigma=1}^{\nu} \left(L_{i\sigma}^{(s)} - \delta_{s\sigma} P_i\right) H_\sigma = 0 \qquad (s = 1, \ldots, \nu),$$

und es muß demnach, da die Größen H_σ von Null verschieden sind, die aus den Koeffizienten dieser Größen gebildete Determinante verschwinden. Man hat also

$$(-1)^\nu \left| L_{i\sigma}^{(s)} - \delta_{s\sigma} P_i \right| = 0 \quad (s, \sigma = 1, \ldots, \nu).$$

Hierin ist eine gleich wichtige zweite Form des Fundamentalsatzes enthalten:

Jedes Koeffizientenprodukt P_i genügt einer Identität:

$$P_i^\nu + \Lambda_1^{(i)} P_i^{\nu-1} + \cdots + \Lambda_k^{(i)} P_i^{\nu-k} + \cdots + \Lambda_\nu^{(i)} = 0, \qquad (\mathrm{K}')$$

wo die $\Lambda_k^{(i)}$ rationale und ganze homogene Formen der Koeffizienten des Formenproduktes C_g von der Dimension k sind. Die rationalen und ganzen Zahlen, die als Koeffizienten in den $\Lambda_k^{(i)}$ auftreten, ändern sich natürlich mit der Wahl von P_i, d. i. der Größen $A_{i_1}^{(1)}, \ldots, A_{i_k}^{(k)}$.

Um dies einzusehen, beachte man nur, daß die $L_{i\sigma}^{(s)}$ rationale und homogene lineare Formen der C_g sind, also jedes Element der Determinante eine ebensolche Form der C_g und P_i ist. Es sind ferner die Elemente der Hauptdiagonale die einzigen, in denen $\delta_{s\sigma}$ von Null verschieden ist, also P_i wirklich vorkommt. Ordnet man also nach Multiplikation mit $(-1)^\nu$ nach fallenden Potenzen von P_i, so ist der Koeffizient von P_i^ν gleich eins, und da die ganze Determinante eine Form ν^{ter} Dimension der C_g und P_i ist, muß der Koeffizient von $P_i^{\nu-k}$ eine Form $\Lambda_k^{(i)}$ mit den angegebenen Eigenschaften sein.

Vollständigen Bereichen entstammende Formen.

§ 8. Der Bereich [A], der die Koeffizienten der betrachteten Formen liefert, soll nun als vollständiger holoider Bereich vorausgesetzt werden. Nach der in Kap. I § 6 gegegebenen Definition gibt es dann, wenn A und B irgend zwei Größen des Bereichs sind, eine gleichfalls dem Bereiche [A] angehörige Größe D, die der größte gemeinschaftliche Teiler

von A und B ist, d. h. die Eigenschaft besitzt, daß ihre sämtlichen Teiler, und nur diese Teiler von A und B sind. Dabei ist selbstverständlich die „Bestimmung" von D im Sinne der absoluten Äquivalenz (Kap. I § 5) zu verstehen.

Ein vollständiger Bereich ist als solcher nur dann wohldefiniert, wenn eine Methode vorliegt, die den größten gemeinschaftlichen Teiler zweier beliebiger Größen des Bereichs in einer endlichen Anzahl von Schritten zu bestimmen gestattet. Dies ist nach den Elementen der Arithmetik insbesondere für den Bereich [1] der Fall und selbstverständlich auch für jeden orthoiden Bereich.

Vor allem nimmt nun der eben behandelte Fundamentalsatz für vollständige Bereiche eine besonders einfache Gestalt an.

Ist nämlich der größte gemeinschaftliche Teiler der in den Identitäten (K) des § 6 auftretenden Größen H_s

$$(H_1, \ldots, H_\nu) \sim H,$$

also

$$H_s = HH_s'$$

und

$$(H_1', \ldots, H_\nu') \sim 1,$$

so kann man den Teiler H aus jenen Identitäten ganz entfernen und erhält

$$H_s' P_i = \sum_{\sigma=1}^{\nu} L_{i\sigma}^{(s)} H_\sigma' \qquad (s = 1, \ldots, \nu).$$

Sei andererseits der größte gemeinschaftliche Teiler der Größen C_g

$$(C_1, \ldots, C_g, \ldots) \sim C,$$

so sind die Größen $L_{i\sigma}^{(s)}$, damit auch die Größen $H_s' P_i$ und endlich

$$(H_1' P_i, \ldots, H_\nu' P_i) \sim P_i$$

durch C teilbar. Wenn also

$$P \sim (P_1, \ldots, P_i, \ldots)$$

den größten gemeinschaftlichen Teiler sämtlicher P_i bezeichnet, so ist P durch C teilbar, und auch C durch P. Letzteres ergibt sich aus der Definition des Produktes, nach welcher

jede Größe C_g eine rationale und ganze homogene, lineare Form der P_i, also durch P teilbar ist. Man hat demnach

$$C \sim P,$$

und damit ergibt sich im Anschlusse an die in § 6 gebrauchten Bezeichnungen, daß die aus den Koeffizienten der Formen F_i gebildeten Produkte $P_i = A_{i_1}^{(1)} \dots A_{i_k}^{(k)}$ und die Koeffizienten C_g des Produktes dieser Formen denselben größten gemeinschaftlichen Teiler haben.

Dieser Satz gibt einen tiefen Einblick in die Struktur des Formenproduktes, vorläufig für vollständige Bereiche, indem er zeigt, daß gewisse Eigenschaften der Koeffizienten des Produktes ungeändert bleiben, wenn man die als Faktoren zu verwendenden Formen, in welcher Weise immer, aus den gegebenen Koeffizienten aufbaut. Dies wird genauer in folgendem Satze ausgesprochen, der weiterhin als Fundamentalsatz für vollständigen Bereichen entstammende Formen citiert werden soll.

Es seien

$$A_0^{(i)}, A_1^{(i)}, \dots, A_g^{(i)}, \dots \qquad (i = 1, 2, \dots, k)$$

k beliebige aus einem vollständigen holoiden Bereiche gewählte Reihen von Größen; es seien ferner

$$U_0^{(i)}, U_1^{(i)}, \dots, U_g^{(i)}, \dots \qquad (i = 1, 2, \dots, k)$$

beliebige Potenzprodukte beliebiger Unbestimmter wo aber die in einer Zeile stehenden voneinander verschieden sind, d. h. nur dann $U_g^{(i)} = U_h^{(i)}$ wird, wenn $g = h$ ist; es sei ferner

$$F_i = \sum_{(g)} A_g^{(i)} U_g^{(i)} \qquad (i = 1, 2, \dots, k)$$

und

$$F = \prod_{i=1}^{k} F_i = \sum_{(h)} C_h V_h,$$

wo die V_h die sämtlichen nach der Multiplikation auftretenden Potenzprodukte der Unbestimmten bedeuten. Dann wird

$$C \sim (C_1, \dots, C_h, \dots)$$

von der Wahl jener Potenzprodukte U völlig unabhängig, eine im Sinne der absoluten Äquivalenzbestimmung unveränderliche (invariante) Größe.

Denn es ist nach dem Vorhergehenden C immer dem größten gemeinschaftlichen Teiler der Größen P_i äquivalent.

Diese selbst treten als Koeffizienten C_h in F auf, wenn man die $U_g^{(i)}$ einfach als durchweg verschiedene Unbestimmte faßt, d. h. die Formen F_i als lineare Formen verschiedener Unbestimmter bildet.

Wenn wir nun vielfach für die Darstellung einer Form die Gestalt $\sum A_g U_g$ statt der ausführlicheren $\sum A_g x_1^{g_1} \dots x_m^{g_m}$ gebrauchen, so wird diese Schreibweise nicht nur als abgekürzte Bezeichnung nützlich sein, sondern zugleich auch darauf hinweisen, daß wir es mit solchen Eigenschaften der Formen zu tun haben, die von der Wahl der Potenzprodukte U_g unabhängig sind. Dabei sind aber immer $U_0, U_1, \dots$ als verschiedene Potenzprodukte anzusehen, sonst wären in der Form die ähnlichen Glieder zu vereinigen, und die Form nicht „aus der Koeffizientenreihe $A_0, A_1, \dots$ aufgebaut".

Eine aus der Koeffizientenreihe $A_0, A_1, \dots, A_g, \dots$ aufgebaute Form soll eben als Bezeichnung für $\sum A_g U_g$ dienen, wenn die verschiedenen Potenzprodukte U_g beliebige bleiben.

§ 9. Eine Form heißt primitiv oder eine Einheitsform, wenn der größte gemeinschaftliche Teiler ihrer Koeffizienten ~ 1 ist*).

---

*) Dabei ist selbstverständlich zu beachten, daß der zu Grunde gelegte vollständige holoide Bereich auch schon Unbestimmte enthalten kann, und diese dann in die Koeffizienten gehören. Wenn sich z. B. später zeigen wird, daß der Bereich $[1, x]$ ein vollständiger ist, so wird

$$x + xy$$

als eine dem Bereiche $[1, x]$ entstammende Form von y nicht primitiv sein, da ihre beiden Koeffizienten gleich x sind, und diese Größe auch als der größte gemeinschaftliche Teiler der beiden Koeffizienten zu be-

Es ist unmittelbar klar, daß die so definierte Eigenschaft der Form wieder ausschließlich eine Eigenschaft ihrer Koeffizienten ist. Die primitiven Formen von der Dimension 0 sind die Einheiten des Bereichs [A].

Ist irgend eine Form

$$F = \sum_{(g)} A_g U_g$$

und

$$(A_0, A_1, \ldots, A_g, \ldots) \sim A,$$

also

$$A_g = A A'_g,$$

$$(A'_0, A'_1, \ldots, A'_g, \ldots) \sim 1,$$

so wird schließlich

$$F = A \sum_{(g)} A'_g U_g,$$

wo der zweite Faktor rechts seiner Bildung gemäß eine primitive Form ist.

Jede dem vollständigen holoiden Bereiche [A] entstammende Form F ist also das Produkt einer dem Bereiche [A] angehörigen Größe und einer primitiven Form. Wir schreiben demgemäß $F = AX$, und nennen gelegentlich X „die primitive Form von F".

Man hat ferner als einfache Folgerung aus dem Fundamentalsatze den wichtigen Satz:

Das Produkt primitiver Formen ist wieder eine primitive Form.

Ist nämlich zuerst für zwei Formen:

$$X = \sum A_g U_g, \quad Y = \sum B_g V_g$$

und

$$(A_0, A_1, \ldots) \sim 1, \quad (B_0, B_1, \ldots) \sim 1,$$

so wird für

$$XY = \sum C_g W_g$$

der größte gemeinschaftliche Teiler C der Koeffizienten C_g nach dem Fundamentalsatze:

---

trachten ist und sich als im Sinne der Äquivalenzbestimmung von 1 verschieden ergibt.

Hingegen ist $x + xy$ als dem Bereiche [1] entstammende Form (der Unbestimmten x, y) primitiv.

$$C \sim (\ldots, A_i B_j, \ldots).$$

Wendet man hier die in Kap. I § 6 gegebenen Sätze über den größten gemeinschaftlichen Teiler an, so wird insbesondere bei wiederholter Benutzung der dort unter I an zweiter Stelle stehenden rekursiven Bestimmung des größten gemeinschaftlichen Teilers C auch der größte gemeinschaftliche Teiler von

$$(A_i B_0, A_i B_1, \ldots, A_i B_j, \ldots) \qquad (i = 0, 1 \ldots).$$

Dieser größte gemeinschaftliche Teiler selbst ist aber:

$$A_i(B_0, B_1, \ldots, B_j, \ldots) \sim A_i,$$

also

$$C \sim (A_0, A_1, \ldots, A_i, \ldots) \sim 1,$$

was zu beweisen war.

Sind nun $X_1, X_2, \ldots, X_k$ primitive Formen, so ist demnach $X_1 X_2$ eine primitve Form, also auch $X_1 X_2 X_3$ und so fort; schließlich also auch das Produkt $X_1 X_2 \ldots X_k$.

§ 10. Ist $F = AX$ und $G = BY$, ferner F durch G teilbar, so ist auch schon A durch B, und X durch Y teilbar. Die Umkehrung des Satzes ist evident; dabei sollen X und Y die primitiven Formen von F und G, ferner A und B Größen aus [A] bedeuten.

Man hat der Annahme nach $F = GH$ und kann wieder $H = CZ$ schreiben; es ist folglich

$$F = AX = (BC)(YZ).$$

Hier ist YZ eine primitive Form, also der größte gemeinschaftliche Teiler der Koeffizienten von F einmal A, dann wieder BC, folglich

$$A \sim BC,$$

mithin A durch BC und daher, wie behauptet, auch durch B teilbar. Andererseits ist BC durch A teilbar, demnach $\frac{BC}{A} = K$ eine Größe des Bereiches [A] und

$$X = Y(KZ)$$

oder auch X durch Y teilbar.

Als einfache Corollare des bewiesenen Satzes seien die vielfach anzuwendenden, unmittelbar evidenten Sätze aufgeführt:

Ist $F = AX$ durch die primitive Form Y teilbar, so ist auch schon die primitive Form von F, d. h. X durch Y teilbar, und

Primitive Formen haben nur primitive Teiler.

§ 11. Es seien nun $(m \geqq n)$

$$F = A_0 x^m + A_1 x^{m-1} + \cdots + A_m,$$
$$G = B_0 x^n + B_1 x^{n-1} + \cdots + B_n$$

zwei Formen des Bereiches $[\mathsf{A}, x]$, also $A_i B_j$ Größen aus dem jetzt als vollständig angenommenen Bereiche $[\mathsf{A}]$, so kann man in vollständiger Analogie zu dem in den Elementen gelehrten Euklidischen Algorithmus, der im Bereiche der rationalen und ganzen Zahlen zur Bestimmung des größten gemeinschaftlichen Teilers führt, mit Hilfe des gewöhnlichen Divisionsverfahrens die folgenden Identitäten aufstellen, die zugleich als Definition der in ihnen auftretenden Formen R dienen:

$$\begin{aligned}
K_0 F &= G Q_1 + R_1 \\
K_1 G &= R_1 Q_2 + R_2 \\
K_2 R_1 &= R_2 Q_3 + R_3 \\
&\cdots\cdots\cdots \\
K_i R_{i-1} &= R_i Q_{i+1} + R_{i+1} \\
&\cdots\cdots\cdots \\
K_{l-1} R_{l-2} &= R_{l-1} Q_l + R_l \\
K_l R_{l-1} &= R_l Q_{l+1}.
\end{aligned} \tag{E}$$

In diesen Identitäten soll K_i diejenige Potenz des höchsten Koeffizienten von R_i bedeuten, die im Sinne des gewöhnlichen Divisionsverfahrens als Faktor der Form R_{i-1} zu verwenden ist, damit man bei Anwendung dieses Verfahrens als Koeffizienten nur Größen des Bereiches $[\mathsf{A}]$ erhalte; Q_{i+1}, R_{i+1} bezeichnen einfach den Quotienten, resp. den Rest, der bei der Division von $K_i R_{i-1}$ durch R_i auftritt. Dann sind $R_1, R_2, \ldots$ Formen des Bereiches $[\mathsf{A}, x]$, deren Grad in Bezug auf x nicht größer als $n - 1$, $n - 2, \ldots$ sein kann. Das Verfahren gelte als abgeschlossen,

wenn R_l der letzte von 0 verschiedene Rest ist; sollte insbesondere das Verfahren zu einem Reste R_l führen, der x nicht mehr enthält und nicht 0 ist, so kann in der letzten Identität $K_l = R_l$, $Q_{l+1} = R_{l-1}$ gesetzt werden; demnach wird $R_{l+1} = 0$.

Ist, wie früher, $F = AX$, $G = BY$ und $R_l = CZ$ (wo, falls R_l die Unbestimmte x nicht enthält, $Z = 1$ zu setzen ist), so ist Z der größte gemeinschaftliche Teiler von X und Y.

Dies wird aus den folgenden einfachen Bemerkungen erschlossen. Jeder gemeinschaftliche Teiler von F und G, also auch von X und Y, ist nach (E) auch in $R_1, R_2, \ldots$, also schließlich auch in R_l enthalten; ein gemeinschaftlicher Teiler von X und Y ist aber primitiv (§ 10) und demnach auch ein Teiler von Z. Umgekehrt ist jeder Teiler von Z ein Teiler von $K_l R_{l-1}$ und, da er primitiv, auch schon ein Teiler von R_{l-1}, ebenso von R_{l-2} und so fort, also schließlich auch von G und F, also auch von X und Y.

Daraus folgt aber unmittelbar die Darstellung des größten gemeinschaftlichen Teilers der Formen $F = AX$, $G = BY$ in der Gestalt

$$(A, B)\ (X, Y),$$

wo (A, B) der Annahme nach bestimmt werden kann, da $[\mathsf{A}]$ ein wohldefinierter vollständiger Bereich ist, und (X, Y) nichts anderes als jene Größe Z ist, deren Bildung der durch (E) definierte Euklidische Algorithmus lehrt.

Man hat daher auch ganz allgemein:

Der einem vollständigen Bereiche $[\mathsf{A}]$ entstammende Formenbereich $[\mathsf{A}, x_1, \ldots, x_m]$ ist abermals ein vollständiger Bereich.

Indem man von $[\mathsf{A}]$ der Reihe nach zu $[\mathsf{A}, x_1]$, $[\mathsf{A}, x_1, x_2]$, ... aufsteigt, erweist sich diese Behauptung als richtig, und wir erhalten zugleich die Vorschrift, nach welcher der größte gemeinschaftliche Teiler zweier beliebigen Formen wirklich gebildet werden kann.

Vollständigen Bereichen zugeordnete orthoide Bereiche.

§ 12. Wenn man (nach Kap. I § 4) von dem Bereiche [A] zu dem zugeordneten orthoiden Bereiche (A) übergeht, soll eine Größe kurz als orthoid oder holoid bezeichnet werden, je nachdem sie dem Bereiche (A) oder [A] angehört, und ebenso soll eine orthoide resp. holoide Form eine solche Form sein, deren Koeffizienten orthoide resp. holoide Größen sind*).

Wenn der Bereich [A] vollständig ist, so kann jede orthoide Größe auf eine kanonische Gestalt gebracht werden; sie kann nämlich durch $\frac{P}{Q}$ dargestellt werden, wo P und Q holoide Größen sind und $(P, Q) \sim 1$ ist. Denn die dem Bereiche (A) angehörige Größe hat jedenfalls die Gestalt $\frac{M}{N}$, wo M und N Größen aus [A] sind. Ist nun $(M, N) \sim D$, also

$$M = DP, \quad N = DQ, \quad (P, Q) \sim 1,$$

so wird in der Tat $\frac{M}{N} = \frac{P}{Q}$.

Nach diesen Festsetzungen hat man den folgenden Satz: Ist [A] ein vollständiger Bereich, sind $A_0, A_1, \ldots, A_k$ Größen dieses Bereichs und ist z eine Größe des Bereiches (A), für welche

$$A_0 z^k + A_1 z^{k-1} + \cdots + A_k = 0 \qquad (1)$$

ist, so muß $A_0 z$ dem Bereiche [A] angehören. Insbesondere ist, wenn A_0 eine Einheit, z selbst schon eine holoide Größe.

Jedenfalls hat z nach dem früheren die Gestalt $\frac{P}{Q}$, wo $(P, Q) \sim 1$; wenn man also in (1) mit Q^k multipliziert, wird

*) Man denke dabei an die adjektivischen Bezeichnungen als rational oder rational und ganz, die in Bezug auf die Bereiche (1) und [1] allgemein gebraucht werden. Entsprechend kann eine orthoide Größe zugleich holoid sein.

$$A_0 P^k + A_1 P^{k-1} Q + \cdots + A_k Q^k = 0;$$

es ist also $A_0 P^k$ durch Q teilbar und, da $(P, Q) \sim 1$, auch A_0 durch Q teilbar, und demnach $A_0 z = \frac{A_0 P}{Q}$ eine holoide Größe.

Dieselbe Gleichung zeigt, daß $A_k Q^k$ und damit auch A_k durch P teilbar ist. Daraus folgt:

Soll eine orthoide Größe $z = \frac{P}{Q}$ der Gleichung (1) genügen, so muß P ein Teiler von A_k, und Q ein Teiler von A_0 sein.

Hat man es mit den Bereichen [1] und (1) zu tun, sind also die Größen $A_0, \ldots, A_k$ rationale und ganze Zahlen, so gibt dieser Satz die vollständige Bestimmung derjenigen rationalen Zahlen, die „Wurzeln" der Gleichung (1) sind; denn jede von 0 verschiedene, rationale und ganze Zahl hat nur eine endliche Anzahl von Teilern, und da der Ausnahmefall $A_k = 0$ leicht vermieden werden kann, gibt eine bestimmte Anzahl von Versuchen sämtliche den Bedingungen genügende rationale Zahlen.

Ist innerhalb des Bereiches (A)

$$z^m + A_1 z^{m-1} + \cdots + A_m =$$
$$= (z^k + M_1 z^{k-1} + \cdots + M_k)(z^{m-k} + N_1 z^{m-k-1} + \cdots + N_{m-k}),$$

sind ferner $A_1, \ldots, A_m$ holoide Größen, so müssen auch die Größen $M_1, \ldots, M_k, N_1, \ldots, N_{m-k}$ holoide Größen sein.

Wendet man nämlich den Kroneckerschen Fundamentalsatz auf das angeführte Produkt an, so genügt jede Größe M_i und N_j (als Koeffizientenprodukt $1 . M_i$ und $1 . N_j$) einer Gleichung, in welcher die höchste Potenz von M_i resp. N_j als Koeffizienten die 1 erhält, während alle anderen Koeffizienten holoide Größen sind. Es müssen also sämtliche M_i und N_j nach dem vorhergehenden Paragraphen holoide Größen sein.

Insbesondere sind im Bereiche (1) mit $A_1, \ldots, A_m$ bei einer Zerlegung von der angegebenen Gestalt auch die Koeffizienten M_i und N_j rationale und ganze Zahlen.

Dieser von Gauß bewiesene Satz*) ist historisch der Ausgangspunkt der allgemeinen Theorie der algebraischen Größen.

Die Resultante.

§ 13. Wir lassen nunmehr die in den letzten Erörterungen festgehaltene Voraussetzung, daß der Bereich [A] vollständig ist, wieder fallen; dies ist um so wichtiger, als die in der Theorie der algebraischen Größen auftretenden Bereiche, wie schon das in Kap. I § 8 und 9 behandelte einfache Beispiel zeigte, im allgemeinen nicht vollständig sind. Der charakteristische Unterschied zwischen beiden Fällen liegt in folgender Tatsache:

Ist A eine Größe des Bereiches [A] und G eine irreduzible Größe des Bereiches [A, x], die kein Teiler von A ist, so wird für vollständige Bereiche mit AF zugleich auch F durch G teilbar, da ja $(A, G) \sim 1$, und demnach aus $(AF, G) \sim G$ auch $(F, G) \sim G$ folgt. Wenn hingegen der Bereich [A] kein vollständiger ist, so kann ganz gut AF durch G teilbar sein, ohne daß dies für F der Fall ist.

Wenn wir wieder das früher zitierte Beispiel des Bereiches $[\sqrt{-5}]$ benutzen, so ist z. B. $2 - \sqrt{-5}$ eine irreduzible Größe und 3 durch diese nicht teilbar, wohl aber $3 \cdot 3$. Daß auch für solche Größen G, die x wirklich enthalten, ähnliche Verhältnisse vorliegen, kann ebenso leicht gezeigt werden. Es ist z. B.

$$G = 3x + (1 - 2\sqrt{-5}),$$

wie man unmittelbar sieht, irreduzibel, und

$$F = (2 + \sqrt{-5})x + (4 - \sqrt{-5})$$

nicht durch G teilbar, wohl aber

$$(2 - \sqrt{-5})F = 9x + 3(1 - 2\sqrt{-5}).$$

Die Frage der Teilbarkeit von F durch G ist demnach so zu verallgemeinern: Gibt es Größen A des Bereiches [A],

*) Disquisitiones Arithmeticae. Art. 42.

so daß AF durch G teilbar wird? Nun ist aber [A] nach Ausschluß der 0 ein in $[A, x_1, \ldots, x_m]$ enthaltener Äquivalenzbereich (Kap. I § 12). Und die Fragestellung lautet demnach: Gibt es eine in Bezug auf den Äquivalenzbereich [A] mit F äquivalente Größe, die durch G teilbar ist?

Die relative Äquivalenz der Größen des Bereiches $[A, x_1, x_2, \ldots, x_m]$ in Bezug auf den Äquivalenzbereich [A] ist aber nichts anderes als die absolute Äquivalenz in jenem Bereiche, der aus $[A, x_1, \ldots, x_m]$ entsteht, wenn wir als Nenner Größen aus [A] zulassen, d. h. in dem aus dem orthoiden Bereiche (A) entstammenden Formenbereiche $[(A), x_1, \ldots, x_m]$. Dieses Resultat kann einfacher gefaßt werden.

Wir gehen von dem holoiden Bereiche [A] zu dem zugeordneten orthoiden Bereiche (A) über und untersuchen die Teilbarkeit der Formen, auch wenn sie holoid sind, in dem erweiterten Formenbereiche $[(A), x_1, \ldots, x_m]$. Dieser Bereich ist vollständig, weil jeder orthoide Bereich, also auch (A), ein vollständiger ist, und es werden daher bei dieser verallgemeinerten Fragestellung die früher entwickelten Methoden zur Anwendung gebracht werden können.

Es kann geradezu als Ziel der Theorie der algebraischen Größen hingestellt werden, den ursprünglichen, den Betrachtungen zu Grunde liegenden Bereich durch neue Begriffsbildungen derart zu erweitern, daß einerseits gewisse im ursprünglichen Bereiche unlösbare Aufgaben im neuen Bereiche eine Lösung erhalten, andererseits aber gewisse Eigenschaften der Größen des ursprünglichen Bereiches im erweiterten Bereiche unverändert bleiben. Zum mindesten sollen jene Gesetze erhalten bleiben, nach denen die Addition und Multiplikation der Größen des ursprünglichen Bereiches zu geschehen hat, so daß diese Operationen für die Größen des ursprünglichen Bereiches auch im erweiterten Bereiche dieselben Größen liefern, wie früher. Wir sagen dann, daß der neue, erweiterte Bereich den ursprünglichen Bereich „enthält“. Dies ist in der Tat beim Übergang von [A] zu (A) der Fall.

Dabei möge aber darauf hingewiesen werden, daß gewisse

andere Eigenschaften der Größen in [A] sich ändern. Denn in (A) ist jede Größe A durch jede von 0 verschiedene Größe B teilbar; die Teilbarkeits-Eigenschaften dieser Größen sind also ganz andere geworden. Dies weist auf eine neue, sehr wichtige Begriffsbildung hin, auf eine solche Erweiterung des Bereiches [A], daß der neue Bereich ein vollständiger sei, und dabei aber auch die auf die Teilbarkeit bezüglichen Eigenschaften der Größen in [A] erhalten bleiben. Dieses Fundamentalproblem erfordert aber weitere Hilfsmittel und wird demnach erst später (Kap. IX) behandelt werden können.

§ 14. Es seien

$$F = A_0 x^m + A_1 x^{m-1} + \cdots + A_m,$$
$$G = B_0 x^n + B_1 x^{n-1} + \cdots + B_n$$

zwei Formen, deren Koeffizienten dem holoiden Bereiche [A] angehören. Geht man in den orthoiden Bereich (A) über, (der auch mit [A] zusammenfallen kann), so sind F und G auch dem Bereiche $[(A), x]$ angehörige Formen und haben als solche einen größten gemeinschaftlichen Teiler. Jede Größe des Bereiches (A) ist der 1 äquivalent; jener größte gemeinschaftliche Teiler ist daher entweder Eins oder eine x enthaltende, wirkliche Form. Die Trennung dieser beiden Fälle führt zu dem wichtigen Grundbegriff der Resultante.

Ist (F, G) einer wirklichen Form von x äquivalent, also

$$(F, G) \sim D = D_0 x^k + D_1 x^{k-1} + \cdots + D_k,$$

so ist

$$F = D\overline{V}, \quad G = -D\overline{U}$$

und

$$-\overline{U} = \overline{P}_0 x^{n-k} + \overline{P}_1 x^{n-k-1} + \cdots + \overline{P}_{n-k},$$
$$\overline{V} = \overline{Q}_0 x^{m-k} + \overline{Q}_1 x^{m-k-1} + \cdots + \overline{Q}_{m-k},$$

wo die Koeffizienten von D, $\overline{U}$ und $\overline{V}$ dem Bereiche (A) angehören. Es muß also

$$\overline{U}F + \overline{V}G = 0$$

sein. Da D zum mindesten vom ersten Grade, also $k \geqq 1$, ist $m - k \leqq m - 1$ und $n - k \leqq n - 1$; soll also (F, G) im Sinne der Äquivalenz von 1 verschieden sein, so muß es zwei Formen

$$-U = P_0 x^{n-1} + \cdots + P_{n-1}$$
$$V = Q_0 x^{m-1} + \cdots + Q_{m-1}$$

geben, deren Koeffizienten nicht sämtlich verschwinden und die der Relation

$$UF + VG = 0$$

genügen. Dieses im wesentlichen von Euler herrührende Verfahren ergibt folgendes System von linearen Gleichungen für die Koeffizienten P und Q:

$$\begin{array}{llr} A_0 P_0 & + B_0 Q_0 & = 0 \\ A_1 P_0 + A_0 P_1 & + B_1 Q_0 + B_0 Q_1 & = 0 \\ \cdots & \cdots & \cdots \\ A_m P_{n-1} + & + B_n Q_{m-1} & = 0, \end{array}$$

wo die allgemeine $k+1^{\text{te}}$ Gleichung des Systems folgendermaßen charakterisiert werden kann:

$$\sum A_i P_r + \sum B_j Q_s = 0$$
$$\left(\begin{array}{c} i=0,1,\ldots,m;\ j=0,1,\ldots,n;\ r=0,1,\ldots,n-1;\ s=0,1,\ldots,m-1 \\ i+r=k,\ j+s=k \end{array}\right)$$

und k der Reihe nach $0, 1, \ldots, m+n-1$ zu setzen ist.

Man hat demnach ein homogenes lineares Gleichungssystem, in dem sowohl die Anzahl der Gleichungen, als die Anzahl der Unbekannten $m+n$ ist; und diese Unbekannten, die Koeffizienten P_r und Q_s, können nur dann nicht sämtlich verschwindende Werte besitzen, wenn die aus den Koeffizienten der Gleichungen gebildete Determinante, die sog. Sylvestersche Determinante*), verschwindet.

---

*) Sylvester, „On a general method of determining by mere inspection the derivations from two equations of any degree", Phil. Mag. 1840, Februar pag. 132. — Gegenüber den unrichtigen Angaben in der „Encyklopädie d. math. Wiss." (Bd. I pag. 246) sei noch bemerkt, daß Richelot in seiner Arbeit aus dem Jahre 1840 „Nota ad theoriam eliminationis pertinens" (Journ. f. Math. Bd. 21) die Sylvesterschen Resultate schon ausdrücklich zitiert. Beinahe vier Jahre später gibt Hesse („Über die Endgleichung etc." Journ. f. Math. Bd. 27 = Werke pag. 83) dieselbe Determinante, erwähnt aber merkwürdigerweise keinen der beiden Vorgänger.

Das Gesetz dieser Determinante

$$R = \begin{vmatrix} A_0 & & & & B_0 & & & \\ A_1 & A_0 & & & B_1 & B_0 & & \\ . & A_1 & . & & . & B_1 & . & \\ . & . & . & A_0 & . & . & . & B_0 \\ . & . & . & A_1 & . & . & . & B_1 \\ A_m & . & . & . & B_n & . & . & . \\ & A_m & . & . & & B_n & . & . \\ & & . & . & & & . & . \\ & & & A_m & & & & B_n \end{vmatrix}$$

ist einfach zu fassen: In der j^{ten} Spalte $(j = 1, \ldots, n)$ stehen nach $j - 1$ Nullen die Elemente $A_0, A_1, \ldots, A_m$, denen wieder $n - j$ Nullen folgen, in der $n + k^{\text{ten}}$ Spalte $(k = 1, \ldots, m)$ nach $k - 1$ Nullen die Elemente $B_0, B_1, \ldots, B_n$ und dann wieder $m - k$ Nullen.

Ist umgekehrt diese Determinante Null, ohne daß A_0 und B_0 zugleich verschwinden, so gibt es bekanntlich Systeme von Werten für die Koeffizienten P_r und Q_s, die nicht sämtlich verschwinden und dem vorgelegten linearen Gleichungssysteme genügen, und zwar auch solche, in denen diese sämtlich rationale und ganze Formen der Größen A_i und B_j sind. Der Relation

$$UF + VG = 0$$

gemäß muß aber VG durch F und UF durch G teilbar sein. Wäre nun $(F, G) \sim 1$, so wäre auch V durch F und U durch G teilbar. Ist nun z. B. A_0 nicht 0, so kann V, eine Form vom höchstens $m - 1^{\text{ten}}$ Grade in x, nur dann durch F teilbar sein, wenn sie identisch verschwindet. Es muß also dann $VG = 0$ sein. Nun kann aber weder V verschwinden, denn es würden dann sämtliche Koeffizienten P_r und Q_s verschwinden, noch $G = 0$ sein, da hieraus $(F, G) \sim F$ folgt und F als Form m^{ten} Grades nicht ~ 1 ist.

Das Verschwinden der Größe R ist demnach die notwen-

dige und hinreichende Bedingung dafür, daß die Formen F und G, in denen A_0 und B_0 nicht zugleich 0 sind, in dem dem orthoiden Bereiche (A) entstammenden Formenbereiche $[(A), x]$ einen im Sinne der Äquivalenz von 1 verschiedenen größten gemeinschaftlichen Teiler besitzen.

§ 15. Die Größe R heißt die Resultante der Formen F und G in Bezug auf die Unbestimmte x, wo diese genauere Beziehung auf x, wenn hierdurch keine Zweideutigkeit entsteht, weggelassen wird. In diesem Falle wählen wir die Bezeichnung

$$\text{Res. } (F, G),$$

wo dann Res. $(G, F) = (-1)^{mn}$ Res. (F, G), wie die definierende Determinante unmittelbar zeigt. Da die Formen F und G auch weitere Unbestimmte enthalten können, wird bei allgemeineren Untersuchungen eine genauere Bezeichnung notwendig, die mit Rücksicht auf spätere Entwicklungen folgendermaßen festgesetzt wird:

$$\text{Res. } \begin{pmatrix} F, & G \\ x, & 1 \end{pmatrix}.$$

Wenn der Bereich [A] selbst schon ein Formenbereich ist, der im allgemeinen dem holoiden Bereiche $[\overline{A}]$ entstammt, also $[A] = \left[[\overline{A}], x_1, x_2, \ldots, x_m\right]$, so zeigt das Verschwinden der Resultante von F und G, wenn A_0 und B_0 nicht zugleich 0 sind, die Existenz eines solchen größten gemeinschaftlichen Teilers:

$$D = D_0 x^k + D_1 x^{k-1} + \cdots + D_k,$$

wo die Größen $D_0, \ldots, D_k$ die Gestalt $\frac{\overline{D}_i}{\overline{E}_i}$ besitzen, $\overline{D}_i$, $\overline{E}_i$ dem Bereiche [A] angehören und wenigstens eine der Größen $\overline{D}_0, \ldots, \overline{D}_{k-1}$, sowie alle Größen E_i von Null verschieden sind. Setzt man also das Produkt der Größen E_i gleich E, so besitzen EF und EG den Teiler

$$D' = D_0' x^k + D_1' x^{k-1} + \cdots + D_k',$$

wo die D_i' Größen des Bereiches [A] sind und wieder wenigstens eine der Größen $D_0', \ldots, D_{k-1}'$ von Null verschieden ist.

Wäre nun $(F, G) \sim 1$ in dem Formenbereiche $\left[(\mathsf{A}), x_1, x_2, \ldots, x_m\right]$, so müßte E durch D' teilbar sein, was unmöglich ist, da E nicht Null ist und die Unbestimmte x nicht enthält.

Ist umgekehrt (F, G) im Sinne der Äquivalenzbestimmung nicht Eins in Bezug auf $\left[(\mathsf{A}), x_1, x_2, \ldots, x_m\right]$, so folgt hieraus unmittelbar ein Teiler von der Gestalt D und das Verschwinden der Resultante.

Man kann demnach die erste Fundamentaleigenschaft der Resultante folgendermaßen fassen:

Sind $F = A_0 x^m + \cdots$, $G = B_0 x^n + \cdots$ zwei Formen, deren Koeffizienten dem holoiden Bereiche [A] entstammende Formen sind, während A_0 und B_0 nicht zugleich Null sind, so ist das Verschwinden der Resultante von F und G die notwendige und hinreichende Bedingung dafür, daß beim Übergang zu den aus dem orthoiden Bereiche (A) entstammenden Formen der größte gemeinschaftliche Teiler von F und G eine die Unbestimmte x wirklich enthaltende Form sei.

Dabei ist nach dem Bisherigen klar, daß der Übergang vom holoiden Bereiche [A] zum orthoiden Bereiche (A) nur dann erforderlich, wenn der Bereich [A] kein vollständiger ist. Wenn [A] ein vollständiger Bereich ist, so gibt es eine Größe A in [A], so daß AF und AG durch eine dem Bereiche [A] entstammende, x enthaltende Form H teilbar sind. Man kann z. B. für A das Produkt der in jenem größten gemeinschaftlichen Teiler von F und G auftretenden Nenner wählen. Dann ist aber F und G durch die primitive Form von H teilbar, und diese ist von 1 verschieden.

Der wesentliche Inhalt der bisher gegebenen Darstellung ist schon in dem folgenden einfachen Satze enthalten:

Die dem orthoiden Bereiche (A) entstammenden in Bezug auf irgend eine Unbestimmte regulären Formen F und G haben dann und nur dann einen von 1 verschiedenen größten gemeinschaftlichen Teiler, wenn ihre Resultante in Bezug auf diese Unbestimmte verschwindet.

Denn in den in Bezug auf diese Unbestimmten geordneten Formen ist weder A_0 noch B_0 gleich Null, und da jeder echte Teiler von F und G wieder regulär sein muß (§ 3 dieses Kapitels), muß auch der größte gemeinschaftliche Teiler, wenn er nicht Eins ist, jene Unbestimmte enthalten.

§ 16. Die zweite Fundamentaleigenschaft der Resultante ist eine einfache Folge ihrer Darstellung als Determinante.

Multipliziert man in der Determinante R (§ 14) die i^{te} Zeile mit x^{m+n-i} und addiert die so erhaltenen Elemente zur unverändert gebliebenen letzten Zeile, so erhält man in dieser der Reihe nach die Elemente

$$Fx^{n-1},\ Fx^{n-2},\ \ldots,\ F,\ Gx^{m-1},\ Gx^{m-2},\ \ldots,\ G,$$

und damit die folgende Darstellung der Größe R:

$$R = G_1F + F_1G,$$

wo G_1 in Bezug auf x höchstens vom $n-1^{ten}$ Grade, und F_1 ebenso höchstens vom $m-1^{ten}$ Grade ist. Dabei sind die Koeffizienten von F_1 und G_1 rationale und ganze Formen der Koeffizienten A und B.

In der Folge sollen durchweg Formen mit dem orthoiden Bereiche (A) angehörigen Koeffizienten zugelassen sein und die Äquivalenzbestimmung sich gleichfalls auf diesen Bereich beziehen. Die erste Fundamentaleigenschaft der Resultante kann dann auch so gefaßt werden, daß aus $R \sim 1$ auch $(F, G) \sim 1$ folgt und umgekehrt.

Ist nun R von 0 verschieden, d. h. $R \sim 1$, so ist auch $(F_1, G_1) \sim 1$; im entgegengesetzten Falle wäre der größte gemeinschaftliche Teiler von F_1, G_1 eine wirkliche Form und doch ein Teiler von R, was unmöglich ist. Auch kann dann weder F_1 noch G_1 Null sein. Wäre z. B. $F_1 = 0$, also $R = G_1F$, so kann G_1 nicht 0 sein, und R wäre durch F teilbar.

Ist $R = 0$, so wird $(F, G) \sim D$ eine Form, die x enthält, und man hat:

$$F = DF', \quad -G = DG', \quad (F', G') \sim 1,$$

oder auch

$$0 = G'F + F'G.$$

Aus irgend einer Relation

$$r = gF + fG,$$

wo f den $m - 1^{\text{ten}}$ und g den $n - 1^{\text{ten}}$ Grad in x nicht überschreiten, beide von 0 verschieden sind und r von x unabhängig ist, ferner $(f, g) \sim 1$ ist, folgt

$$r \sim R,$$

d. h. die Größe r kann genau so wie R benutzt werden, um zu entscheiden, ob (F, G) die Unbestimmte x wirklich enthält. Zum Beweise bemerke man, daß aus

$$r = gF + fG, \quad R = G_1F + F_1G$$

weiter auch

$$(gF_1 - fG_1)F = rF_1 - Rf$$

folgt, wo die rechte Seite in x höchstens vom $m - 1^{\text{ten}}$ Grade ist und doch durch F teilbar sein soll. Es muß also

$$rF_1 - Rf = 0,$$
$$gF_1 - fG_1 = 0$$

sein. Dann folgt unmittelbar aus $r = 0$ auch $R = 0$; und umgekehrt aus $R = 0$, da r durch (F, G) teilbar ist und diese Größe jetzt x enthält, auch $r = 0$; und dies ist die Bedeutung der Äquivalenz $r \sim R$.

§ 17. Ist wieder $(F, G) \sim D$, also $\left(\frac{F}{D}, \frac{G}{D}\right) \sim 1$, so gibt es eine Größe R', die Resultante von $\frac{F}{D}$ und $\frac{G}{D}$, die nicht verschwindet und x nicht enthält, so daß

$$DR' = UF + VG$$

wird; d. h. der größte gemeinschaftliche Teiler von F und G kann nach Multiplikation mit einer x nicht enthaltenden Größe als homogene lineare Form von F und G dargestellt werden.

Dabei können R' und die Koeffizienten von U und V durch einen passend gewählten Faktor in holoide Formen verwandelt werden.

Insbesondere wird dieses Resultat zur Verwendung gelangen, wenn der ursprüngliche Bereich [A] ein vollständiger ist, da man dann D auch in derjenigen Gestalt schreiben kann, die für (F, G) sich innerhalb des [A] entstammenden Formenbereichs ergibt.

Daß man auch hier nicht weitergehen kann, d. h. D nicht selbst als homogene lineare Form von F und G darstellen kann, zeigt ein einfachstes Beispiel, wo der Bereich [1] zu Grunde gelegt ist. Die Formen $x + 2$ und $x + 4$ haben den größten gemeinschaftlichen Teiler 1; und es ist

$$2 = (x + 4) - (x + 2);$$

eine Relation von der Form

$$1 = U(x + 2) + V(x + 4)$$

hingegen ist unmöglich. Denn es müßte das von x unabhängige Glied rechts die Gestalt $2a + 4b$ besitzen und gleich eins sein; also 1 durch 2 teilbar sein.

Die Resolventenform eines Formensystems.

§ 18. Die folgende Untersuchung wird sich am einfachsten gestalten, wenn wir die zu betrachtenden Formen als einem vollständigen holoiden Bereiche [A] entstammend annehmen. Um die Resultate auf andere Fälle anzuwenden, wird nur zu bemerken sein, daß dann sämtliche Koeffizienten auch in dem zugeordneten orthoiden Bereiche (A) enthalten sind, und da jeder orthoide Bereich auch vollständig ist, wird dadurch eine Fassung des Ergebnisses erreicht, die auch dann gültig bleibt, wenn der zu Grunde liegende Bereich [A] ein unvollständiger holoider Bereich ist.

Seien nun

$$F_j(x_1, x_2, \ldots, x_m) \qquad (j = 1, \ldots, k)$$

k Formen, die dem vollständigen holoiden Bereiche [A] entstammen. Um zu entscheiden, ob der größte gemeinschaftliche Teiler dieser Formen selbst dem Bereiche [A] angehört oder aber wenigstens eine der Unbestimmten $x_1, \ldots, x_m$ wirk-

lich enthält, wird es am einfachsten sein, die Formen F_j einer linearen Transformation mit rationalen und ganzen Koeffizienten zu unterwerfen, deren Determinante gleich Eins ist (Kap. II, § 19) und sämtliche Formen in solche überführt, die in Bezug auf die neuen Unbestimmten regulär sind. Die fragliche Eigenschaft wird durch diese lineare Transformation nicht gestört; denn der größte gemeinschaftliche Teiler der transformierten Formen entsteht, wie unmittelbar evident, durch Anwendung derselben linearen Transformation auf den größten gemeinschaftlichen Teiler der ursprünglichen Formen. Da aber jeder Teiler einer regulären Form wieder regulär ist, reduziert sich die Frage nun dahin, ob jene Formen überhaupt einen solchen gemeinschaftlichen Teiler besitzen, der y_1 enthält. Diese Transformation, die nach dem von Kronecker gebrauchten Ausdruck das Formensystem „von Zufälligkeiten befreit", ist nichts anderes, als das, was in geometrischer Sprachweise als eine Affinität bezeichnet wird, und zwar eine solche, bei welcher die „im Unendlichen liegenden" Elemente für die zur Entscheidung vorliegenden Fragen nicht weiter in Betracht kommen.

Um die Bezeichnungen nicht zu kompliziert zu gestalten, mögen die Formen F_j und die Unbestimmten x_i schon die transformierten Formen und Unbestimmten sein.

Sind nun u_j und u_i' $(j = 1, \ldots, k)$ zwei neue Reihen von Unbestimmten, so werden die Formen

$$\sum_{j=1}^{k} F_j u_j \quad \text{und} \quad \sum_{j=1}^{k} F_j u_j'$$

dann und nur dann einen x_1 enthaltenden gemeinschaftlichen Teiler besitzen, wenn dies in Bezug auf die Formen F_j der Fall ist. Die formale Zusammenfassung der Formen F_j mit Hilfe der neuen Unbestimmten u_j und u_j' ist von weittragendster Bedeutung; zuerst von Kronecker*) angewendet, soll sie als Kroneckersches Eliminationsprinzip bezeichnet werden.

*) Festschrift, § 10.

Auch diese neuen Formen mögen als Formen der Unbestimmten $x_1, \ldots, x_m$ aufgefaßt werden, deren Koeffizienten aber jetzt dem vollständigen holoiden Bereiche

$$[\mathsf{A}, u_1, \ldots, u_k, u_1', \ldots, u_k']$$

angehören. Als solche sind sie aber mit $F_1, \ldots, F_k$ zugleich regulär, d. h. der Koeffizient der höchsten Potenz von x_i ist eine von den Unbestimmten $x_1, \ldots, x_m$ unabhängige Größe. Es ist demnach

$$\text{Res.}\left(\begin{matrix}\sum F_j u_j, & \sum F_j u_j' \\ x_1\ , & 1\end{matrix}\right) = R_0 U_0 + R_1 U_1 + \cdots,$$

wo die $U_0, U_1, \ldots$ die verschiedenen Potenzprodukte der Unbestimmten u und u' bedeuten, während die $R_0, R_1, \ldots$ Größen des Bereichs $[\mathsf{A}, x_2, \ldots, x_m]$ sind, und das Verschwinden von $R_0, R_1, \ldots$ wird die notwendige und hinreichende Bedingung für die Existenz eines gemeinschaftlichen Teilers der Formen F_j, der x_1 wirklich enthält.

Sei nun

$$(F_1, \ldots, F_k) \sim D, \quad F_j = \bar{F}_j D,$$

also

$$(\bar{F}_1, \ldots, \bar{F}_k) \sim 1$$

und weiter

$$\text{Res.}\left(\begin{matrix}\sum \bar{F}_j u_j, & \sum \bar{F}_j u_j' \\ x_1\ , & 1\end{matrix}\right) = F_1^{(1)} U_0 + F_2^{(1)} U_1 + \cdots,$$

so können die Größen $F_1^{(1)}, F_2^{(1)}, \ldots$ nicht sämtlich verschwinden. Nach der in § 16 bewiesenen zweiten Fundamentaleigenschaft der Resultanten ist nun

$$F_1^{(1)} U_0 + F_2^{(1)} U_1 + \cdots = G_1 \sum \bar{F}_j u_j + H_1 \sum \bar{F}_j u_j',$$

und wenn man die Koeffizienten der verschiedenen Potenzprodukte U_l vergleicht, wird jede Größe $F_{j_1}^{(1)}$ eine homogene lineare Form der $\bar{F}_j$ oder bei Benutzung der in Kap. I, § 10 definierten Bezeichnung:

$$F_{j_1}^{(1)} \equiv 0 \pmod{\bar{F}_1, \ldots, \bar{F}_k}, \qquad (j_1 = 1, \ldots, k_1)$$

und demnach

$$DF_{j_1}^{(1)} \equiv 0 \pmod{F_1, \ldots, F_k} \qquad (j_1 = 1, \ldots, k_1).$$

Dabei sind $F_{j_1}^{(1)}$ dem holoiden Bereiche [A] entstammende Formen von $x_2, \ldots, x_m$.

Die Formen $F_{j_1}^{(1)}$ können wieder als regulär in Bezug auf $x_2, \ldots, x_m$ vorausgesetzt werden. Wäre dies nicht der Fall, so genügte eine lineare Transformation $T^{(1)}$ der Unbestimmten $x_2, \ldots, x_m$ mit rationalen und ganzen Koeffizienten, deren Determinante gleich Eins ist, um reguläre Formen zu erhalten. Diese Transformation kann aber gleich vom Beginne ab an den Formen F_j nach jener Transformation ausgeführt werden, die diese Formen zu solchen umgestaltete, die regulär sind. Dabei ändern sich die bisherigen Resultate nur insofern, als auch die weiter definierten Größen $D, F_1^{(1)}, F_1^{(2)}, \ldots$ schon durch die lineare Transformation $T^{(1)}$ umgestaltet erscheinen.

Wenn man mit den Formen

$$F_{j_1}^{(1)}(x_2, \ldots, x_m) \qquad (j_1 = 1, \ldots, k_1)$$

genau ebenso verfährt, sei:

$$\left(F_1^{(1)}, \ldots, F_{k_1}^{(1)}\right) \sim D^{(1)},$$

$$F_{j_1}^{(1)} = D^{(1)} \bar{F}_{j_1}^{(1)},$$

$$\text{Res.}\begin{pmatrix} \sum \bar{F}_{j_1}^{(1)} u_{j_1} & , & \sum \bar{F}_{j_1}^{(1)} u'_{j_1} \\ x_2 & , & 1 \end{pmatrix} = F_1^{(2)} U_0^{(1)} + F_2^{(2)} U_2^{(1)} + \cdots,$$

und es wird für das Formensystem

$$F_{j_2}^{(2)}(x_3, \ldots . x_m) \qquad (j_2 = 1, \ldots, k_2)$$

wieder

$$D^{(1)} F_{j_2}^{(2)} \equiv 0 \quad \left(\text{mod. } F_1^{(1)}, \ldots, F_{k_1}^{(1)}\right),$$

also schließlich

$$DD^{(1)} F_{j_2}^{(2)} \equiv 0 \pmod{F_1, \ldots, F_k}.$$

Auf diese Weise fortfahrend, erhält man aus dem Formensystem

$$F_{j_{h-1}}^{(h-1)}(x_h, \ldots, x_m) \qquad (j_{h-1} = 1, \ldots, k_{h-1}),$$

wenn

$$\left(F_1^{(h-1)}, \ldots, F_{k_{h-1}}^{(h-1)}\right) \sim D^{(h-1)}$$

und

$$F_{j_{h-1}}^{(h-1)} = D^{(h-1)} \overline{F}_{j_{h-1}}^{(h-1)}$$

gesetzt wird,

$$\text{Res.}\begin{pmatrix} \sum \overline{F}_{j_h-1}^{(h-1)} u_{j_{h-1}}, & \sum \overline{F}_{j_h-1}^{(h-1)} u'_{j_{h-1}} \\ x_h, & 1 \end{pmatrix} =$$

$$= F_1^{(h)} U_0^{(h-1)} + F_2^{(h)} U_1^{(h-1)} + \cdots;$$

also allgemein eine Reihe von Formensystemen:

$$F_{j_h}^{(h)}(x_{h+1}, \ldots, x_m), \qquad (j_h = 1, \ldots k_h),$$

in denen die Unbestimmten $x_1, \ldots, x_h$ nicht mehr vorkommen; während die Formen in Bezug auf $x_{h+1}, \ldots, x_m$ regulär sind, also diese Unbestimmte wirklich enthalten, oder aber von der Dimension 0 sind, d. h. von allen Unbestimmten frei sind. Solange dies nicht mit allen Formen der Fall ist, kann das angegebene Verfahren fortgesetzt werden; man gelangt aber, wenn nicht früher, jedenfalls nach m Schritten, im allgemeinen nach r Schritten zu Größen

$$F_{j_r}^{(r)} \qquad (j_r = 1, \ldots, k_r),$$

die von den Unbestimmten ganz frei sind, also Größen des Bereichs [A] werden.

Setzt man noch

$$D^{(h)} \sim \left(F_1^{(h)}, F_2^{(h)}, \ldots, F_{k_h}^{(h)}\right)$$

und insbesondere für $h = r$

$$F_{j_r}^{(r)} = D^{(r)} C_{j_r} \qquad (j_r = 1, \ldots, k_r),$$

so erhält man schließlich

$$DD^{(1)} \ldots D^{(r)} C_{j_r} \equiv 0 \pmod{F_1, \ldots, F_k} \qquad (\overline{\mathrm{R}})$$

oder, wenn man mit Hilfe der neuen Unbestimmten $w_1, w_2, \ldots$ zusammenfaßt:

$$DD^{(1)} \ldots D^{(r)} \sum_{j_r=1}^{k_r} C_{j_r} w_{j_r} \equiv 0 \pmod{F_1, \ldots, F_k}, \qquad (\mathrm{R})$$

wo $D^{(h)}$ $(h = 1, \ldots, r-1)$ eine in Bezug auf $x_{h+1}, \ldots, x_m$ reguläre Form der Unbestimmten $x_{h+1}, \ldots, x_m$ ist, während $D^{(r)}$, C_{j_r} Größen des Bereichs [A] bedeuten und $1 \leqq r \leqq m$ wird.

Die in (R) links stehende Form soll der wichtigen Beziehung wegen, in der sie zur Theorie der Gleichungssysteme steht, die Resolventenform des Formensystems F_i heißen. Dabei sei besonders erwähnt, daß die in (R) ausgedrückte Eigenschaft dieser Resolventenform auch dann besteht, wenn die Formen zum Teil oder alle von der Dimension 0 sind; für den letzten Fall ist das Resultat allerdings ein triviales. Ist nämlich

$$(A_1, \ldots, A_k) \sim D, \quad A_i = DC_i,$$

so wird aus (R) die selbstverständliche Beziehung

$$D \sum_{i=1}^{k} C_i w_i = \sum_{i=1}^{k} A_i w_i.$$

Man sieht ferner, daß (R) auch dann gültig bleibt, wenn die Formen F_i in ihrer ursprünglichen Gestalt beibehalten werden, mit der einzigen Beschränkung, daß die Formen $D, D^{(1)}, \ldots, D^{(r-1)}$ noch immer wirkliche Formen sind, aber nicht mehr jene oben angegebene spezielle Gestalt besitzen. Um dies einzusehen, hat man nur in der auf die transformierten Formen bezüglichen Kongruenz (R) wieder die reziproke Transformation auszuführen.

Ist endlich der holoide Bereich [A] nicht vollständig, so kann man die Kongruenz (R) oder die entsprechende Identität

$$D D^{(1)} \dots D^{(r)} \sum_{i_r=1}^{k_r} C_{j_r} w_r = \sum_{i=1}^{r} G_i F_i$$

jedenfalls in dem entsprechenden orthoiden Bereich (A) aufstellen; jede Form $D^{(h)}$ hat nun die Gestalt $\frac{\overline{D}^{(h)}}{A_h}$, wo schon $\overline{D}^{(h)}$ dem holoiden Bereiche [A] angehörende Koeffizienten besitzt und kein A_h Null wird. Multipliziert man daher mit einem solchen Vielfachen von $A_1 A_2 \dots A_k$, daß auch die Größen C_{j_r} und die Koeffizienten von G_i holoid werden, so erhält man für unvollständige holoide Bereiche die entsprechende Kongruenz

$$A \overline{D} \overline{D}^{(1)} \dots \overline{D}^{(r)} \sum_{j_r=1}^{k_r} \overline{C}_{j_r} w_{j_r} \equiv 0 \pmod{F_1, \dots, F_k}, \qquad (\overline{\mathrm{R}})$$

wo die links stehende Größe, also auch ihre sämtlichen Faktoren, von 0 verschieden sind.

Das Problem der Theorie der Gleichungen.

§ 19. Sind wieder $F_j(x_1, \dots, x_m) = 0 \quad (j = 1, \dots, k)$ dem holoiden Bereiche [A] entstammende Formen, so kann das allgemeine Problem, das in der sogenannten Theorie der Gleichungen und Gleichungssysteme auftritt und — wie besonders betont werden soll — in dieser Fassung auch die sogenannten diophantischen Gleichungen mit enthält,*) in folgender Weise formuliert werden:

(a) Es sollen alle jene dem holoiden Bereiche [A] angehörigen Wertsysteme $x_i = \xi_i (i = 1, 2, \dots, m)$ bestimmt werden, für welche $F_j(\xi_1, \dots, \xi_m) \; (j = 1, \dots, k)$ gleich Null wird.

*) In unsrem Gedankengange sogar eigentlich hier nur diophantische Gleichungen. Das klassische Gleichungsproblem ergibt sich, wenn man als holoiden Bereich die Gesamtheit der komplexen Zahlen zu Grunde legt.

Dabei sind wir von den „Formen" zu den „ganzen Funktionen" übergegangen; dieser Übergang ist in der Natur der Sache begründet; denn ein solches Wertsystem ξ_i gibt eine fundamentale Eigenschaft der ganzen Funktion F, nämlich eine ihrer „Nullstellen". Trotzdem sei der prinzipiellen Auffassung wegen sogleich bemerkt, daß dasselbe Problem auch so gefaßt werden kann, daß wir vollständig auf dem Gebiete der Theorie der Formen bleiben. Diese Fassung lautet:

(b) Es sollen alle jene dem holoiden Bereiche [A] angehörigen Wertsysteme $\xi_i (i = 1, \ldots, m)$ bestimmt werden, für welche

$$F_j(x_1, \ldots, x_m) \equiv 0 \quad (\text{mod. } x_1 - \xi_1, x_2 - \xi_2, \ldots, x_m - \xi_m) \qquad (j = 1, \ldots, k)$$

wird.

Daß die in (a) und (b) ausgesprochene Eigenschaft der Wertsysteme ξ_i dieselbe ist, erschließt man unmittelbar, wenn man die Form

$$F_j(x_1, \ldots, x_m) = F_j(\xi_1 + x_1 - \xi_1, \ldots, \xi_m + x_m - \xi_m)$$

nach den Potenzprodukten der $x_1 - \xi_1, \ldots, x_m - \xi_m$ entwickelt und das Resultat in der Gestalt

$$F_j(x_1, \ldots, x_m) \equiv F_j(\xi_1, \ldots, \xi_m) \quad (\text{mod. } x_1 - \xi_1, \ldots, x_m - \xi_m)$$

schreibt. Man sieht unmittelbar, daß die der Bedingung (a) genügenden Wertsysteme ξ_i auch der Bedingung (b) genügen. — Ist umgekehrt ξ_i ein der Bedingung (b) genügendes Wertsystem, so wird

$$F_j(x_1, \ldots, x_m) \equiv 0 \quad (\text{mod. } x_1 - \xi_1, \ldots, x_m - \xi_m)$$

oder ausführlich geschrieben:

$$F_j(x_1, \ldots, x_m) = G_1(x_1 - \xi_1) + \cdots + G_m(x_m - \xi_m),$$

wo man F_j und die Formen G nach den Potenzprodukten der $x_1 - \xi_1, \ldots, x_m - \xi_m$ geordnet denken kann. Dann ist das Glied mit dem Potenzprodukte von der Dimension 0 rechts gleich 0; es muß also auch $F_j(\xi_1, \ldots, \xi_m) = 0$ sein.

Jedes solches Wertsystem $\xi_1, \ldots, \xi_m$ heißt eine „Lösung des Gleichungssystems $F_j = 0$“ oder auch „Wurzel“, resp. „Wurzelsystem“ davon. Die Unbestimmten $x_1, \ldots, x_m$ sind dann die in dem Gleichungssysteme auftretenden „Unbekannten“.

Die Dimension einer Gleichung $F = 0$, sowie ihr Grad in Bezug auf eine Unbekannte x_i sind nichts anderes, als die für die Form F ebenso benannten Zahlen.

Für die Gleichung m^{ten} Grades mit einer Unbekannten

$$F(x) = A_0 x^m + A_1 x^{m-1} + \cdots + A_m = 0$$

hat man folgende elementare Sätze, die fortwährend zur Anwendung gelangen.

I. Die Gleichung $F(x) = 0$ hat dann und nur dann die Wurzel ξ, wenn die Form $F(x)$ durch $x - \xi$ teilbar ist.

Es ist dies nichts anderes, als der Satz von der Gleichwertigkeit der Bedingungen (a) und (b) für den nun betrachteten speziellen Fall.

II. Innerhalb des holoiden Bereiches [A], dem auch die (nicht durchwegs verschwindenden) Koeffizienten der Gleichung $F(x) = 0$ angehören, kann diese nie mehr als m verschiedene Wurzeln besitzen.

Wären $\eta_i (i = 1, \ldots, m+1)$ $m+1$ verschiedene Werte, die der Gleichung genügen, so würde

$$A_0 \eta_i^m + \cdots + A_m = 0 \qquad (i = 1, \ldots, m+1)$$

ein homogenes lineares Gleichungssystem für $A_0, \ldots, A_m$ darstellen, und da die Determinante dieses Gleichungssystems

$$[\eta_i^m] = \prod_{\substack{r,s \\ r<s}} (\eta_r - \eta_s) \qquad \left(r, s = 1, \ldots, m+1\right)$$

nach Kap. II, § 11 von 0 verschieden ist, würde hieraus im Gegensatz zur Annahme folgen, daß sämtliche Koeffizienten der Gleichung verschwinden.

§ 20. Wendet man nun auf das Formensystem oder — wie wir uns jetzt auch ausdrücken wollen — auf das Gleichungssystem $F_j = 0$ eine lineare Transformation an, deren Koeffizienten

rationale und ganze Zahlen sind, und deren Determinante gleich Eins, so erhält man das transformierte Gleichungssystem $\bar{F}_j = 0$, und es ist unmittelbar evident, daß das ursprüngliche und das transformierte Gleichungssystem zugleich als aufgelöst zu betrachten ist, da der Übergang von den Lösungen des einen zu den Lösungen des anderen durch ein lineares Gleichungssystem vermittelt wird. Und zwar ist, wenn $\xi_1, \ldots, \xi_m$ irgend eine Lösung von $F_j = 0$, ein bestimmtes System von rationalen und ganzen, homogenen und linearen Formen der ξ_i eine Lösung von $\bar{F}_j = 0$ und umgekehrt.

Wir können demnach das Gleichungssystem $F_j = 0$ schon genau so „vorbereitet" denken, wie dies im Vorhergehenden für die Aufstellung der Resolventenform geschah, und überhaupt die auf diese bezüglichen Resultate zur Anwendung bringen. Dabei tritt die weitere Vereinfachung ein, daß wir uns durchweg in dem Formenbereiche bewegen können, der dem orthoiden Bereiche (A) entstammt; denn jeder Lösung der Gleichung

$$\sum \frac{A'_g}{E'_g} x_1^{g_1} \ldots x_m^{g_m} = 0 \quad \text{oder} \quad \sum \frac{A_g}{E} x_1^{g_1} \ldots x_m^{g_m} = 0$$

entspricht auch der Gleichung mit holoiden Koeffizienten

$$\sum A_g x_1^{g_1} \ldots x_m^{g_m} = 0$$

und umgekehrt; denn dabei ist E das Produkt der E'_g und mit diesen von Null verschieden. Soweit demnach bei weiterer Behandlung des Problems Gleichungen mit orthoiden Koeffizienten auftreten, können diese mit gemeinschaftlichem Nenner geschrieben werden, und dann der Nenner ganz wegbleiben. Dies soll im folgenden überall als geschehen angenommen werden.

Dann zeigt die Kongruenz (R) des § 18 unmittelbar, daß jede Lösung des Gleichungssystems $F_j = 0$ auch Lösung einer der Gleichungen

$$D = 0, \quad D^{(1)} = 0, \quad \ldots, D^{(r-1)} = 0$$

sein muß.

Jede Lösung von $D = 0$ wird, da F_j nach Multiplikation mit einer von Null verschiedenen holoiden Größe durch D teilbar wird, auch eine Lösung des Systems $F_j = 0$. Im allgemeinen wird aber D eine holoide Größe sein, welche die Unbestimmten x überhaupt nicht enthält und auch nicht Null ist; d. h. die Gleichung $D = 0$ hat dann gar keine Lösung.

Ist im allgemeinen $D^{(h)}$ eine wirkliche Form der Unbestimmten $x_{h+1}, \ldots, x_m$, und $\xi_{h+1}, \ldots, \xi_m$ eine Lösung der Gleichung $D^{(h)} = 0$, so verschwinden beim Einsetzen dieser Werte die ganzen Funktionen $F_{j_h}^{(h)}(j_h = 1, \ldots, k_h)$. Die Formen

$$\overline{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$$

besitzen demgemäß einen größten gemeinschaftlichen Teiler $G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m)$*).

---

*) Die Bezeichnung $G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m)$ soll darauf hinweisen, daß $G_1^{(h)}$ eine Form von x_h ist, deren Koeffizienten durch das Wertsystem $\xi_{h+1}, \ldots, \xi_m$ bestimmt sind, ohne daß es eine Form

$$\Gamma(x_h, x_{h+1}, \ldots, x_m)$$

gäbe, aus der $G_1^{(h)}$ ausnahmslos entsteht, wenn

$$x_{h+1} = \xi_{h+1}, \ldots, x_m = \xi_m$$

gesetzt wird. Wie solche Ausnahmen entstehen, möge folgendes einfache Beispiel zeigen.

Der größte gemeinschaftliche Teiler von

$$(x - a)(x - b) \quad \text{und} \quad (x - a + y - z)(x - b + z),$$

wo die Werte von y und z der Gleichung $y - z = 0$ genügen, ist $x - a$, wenn $y = z \neq 0$, und $(x - a)(x - b)$, wenn $y = z = 0$.

Der größte gemeinschaftliche Teiler der Formen

$$\overline{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$$

ist eine im Sinne der absoluten Äquivalenz bestimmte Form

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m),$$

die aber nicht in der Gestalt $G_1^{(h)}(x_h, \xi_{h+1}, \ldots, \xi_m)$ geschrieben werden darf. Dabei ist der Umstand, daß $G_1^{(h)}$ eben nur im Sinne der absoluten Äquivalenz bestimmt ist, ohne Belang; um eine vollständige Bestimmung von $G_1^{(h)}$ zu erlangen, kann man z. B. festsetzen, daß der Koeffizient der höchsten Potenz von x_h immer gleich 1 zu wählen ist.

Ist weiter $x_h = \xi_h$ irgend eine Lösung der Gleichung

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m) = 0,$$

so verschwinden die Funktionen $\overline{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$ dann und nur dann, wenn für x_h eine Größe ξ_h gesetzt wird*). Also verschwindet

$$F_{j_{h-1}}^{(h-1)} = D^{(h-1)} \overline{F}_{j_{h-1}}^{(h-1)}$$

wieder nur in diesem Falle (die entsprechenden Lösungen mögen Lösungen erster Art heißen) oder aber, wenn $D^{(h-1)} = 0$ wird; wo aber die aus der letzteren Möglichkeit folgenden Lösungen nicht weiter in Betracht kommen, da sie schon bei der Diskussion der Gleichung $D^{(h-1)} = 0$ zur Darstellung kamen.

Wenn nun die Gleichungen $F_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m) = 0$ keine Lösung erster Art besitzen, so können auch die Formen

$$\overline{F}_{j_{h-2}}^{(h-2)}(x_{h-1}, \xi_h, \ldots, \xi_m)$$

für keinen Wert von ξ_h einen gemeinschaftlichen Faktor, also auch die Gleichungen $\overline{F}_{j_{h-2}}^{(h-2)} = 0$ keine Lösung besitzen. Für

$$F_{j_{h-2}}^{(h-2)} = D^{(h-2)} \overline{F}_{j_{h-2}}^{(h-2)}$$

kann also $x_{h-1} = \xi_{h-1}, \ldots, x_m = \xi_m$ nur dann eine Lösung sein, wenn sie auch die Gleichung $D^{(h-2)} = 0$ befriedigt, was wieder nicht weiter in Betracht kommt.

---

*) Ist nämlich ξ_h eine Wurzel der Gleichung

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m) = 0,$$

so ist $G_1^{(h)}$ durch $x_h - \xi_h$ teilbar, also auch $\overline{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$ durch $x_h - \xi_h$ teilbar, demnach $\overline{F}_{j_{h-1}}^{(h-1)}(\xi_h, \xi_{h+1}, \ldots, \xi_m) = 0$.

Bestehen umgekehrt die letzteren Gleichungen, so ist jedes

$$\overline{F}_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m)$$

durch $x_h - \xi_h$ teilbar, also auch der größte gemeinschaftliche Teiler

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m);$$

demnach ist in diesem Falle endlich auch

$$G_1^{(h)}(\xi_h \mid \xi_{h+1}, \ldots, \xi_m) = 0.$$

So weiter schließend sieht man, daß dem ursprünglichen Gleichungssystem nur solche Lösungen von $D^{(h)} = 0$ entsprechen, die auch die Gleichung

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m) = 0$$

befriedigen und mit dieser zugleich daher auch eine Lösung des Systems

$$F_{j_{h-1}}^{(h-1)}(x_h, \xi_{h+1}, \ldots, \xi_m) = 0$$

sind. Dabei sind jene Lösungen, die sich schon aus $D^{(h-1)} = 0$ ergeben, unberücksichtigt geblieben.

Ist nun $\xi_h, \ldots, \xi_m$ eine solche Lösung, so besitzen die Formen

$$\overline{F}_{j_{h-2}}^{(h-2)}(x_{h-1}, \xi_h, \ldots, \xi_m)$$

wieder einen gemeinschaftlichen Faktor:

$$G_2^{(h)}(x_{h-1} \mid \xi_h, \ldots, \xi_m).$$

Ist ferner wieder ξ_{h-1} eine Lösung der entsprechenden Gleichung, so kann man ebenso weitergehen und erhält schließlich diejenigen Lösungen des Gleichungssystems $F_j = 0$, die zugleich der Gleichung $D^{(h)} = 0$ genügen, durch folgende Kette von Gleichungen.:

$$\begin{aligned} D^{(h)}(x_{h+1}, x_{h+2}, \ldots, x_m) &= 0 \\ G_1^{(h)}(x_h \mid x_{h+1}, \ldots, x_m) &= 0 \\ G_2^{(h)}(x_{h-1} \mid x_h, \ldots, x_m) &= 0 \\ \cdots\cdots\cdots\cdots & \\ G_h^{(h)}(x_1 \mid x_2, \ldots, x_m) &= 0, \end{aligned}$$

wo $G_i^{(h)}$ seiner Bildung nach eine reguläre Form von x_{h-i+1} ist.

Die dadurch erreichte Vereinfachung des Gleichungsproblems ist eine wesentliche. Man hat es dabei immer nur mehr mit einzelnen Gleichungen zu tun; zuerst mit einer solchen, die noch eventuell mehrere Unbekannte enthält. Ist $\xi_h, \ldots, \xi_m$ irgend eine Lösung der ersten Gleichung,

so muß das entsprechende ξ_{h-1} der Gleichung mit einer Unbekannten

$$G_1^{(h)}(x_h \mid \xi_{h+1}, \ldots, \xi_m) = 0,$$

dann wieder ein entsprechendes ξ_{h-2} der Gleichung

$$G_2^{(h)}(x_{h-1} \mid \xi_h, \ldots, \xi_m) = 0$$

genügen und so fort. Man erhält dann und nur dann eine Lösung, wenn die so interpretierten Gleichungen sämtlich lösbar sind.

§ 21. Die Gesamtheit der Lösungen des Gleichungssystems $F_j = 0$ kann demnach, soweit Lösungen überhaupt vorhanden sind, nach den Gleichungen $D^{(h)} = 0$, deren einer jede Lösung genügt, in verschiedene Komplexe geordnet werden, wobei es allerdings nicht ausgeschlossen ist, daß dieselbe Lösung zu gleicher Zeit verschiedenen Komplexen angehört.

Der der Gleichung $D^{(h)} = 0$ zugehörige Komplex von Lösungen wird dadurch charakterisiert, daß solche Lösungen, für welche $x_{h+1} = \xi_{h+1}, \ldots, x_m = \xi_m$ wird, nur in endlicher Zahl vorhanden sein können; es ist dies eine unmittelbare Folgerung aus dem in § 19 bewiesenen elementaren Satze, daß eine Gleichung m^{ten} Grades mit einer Unbekannten, deren Koeffizienten Größen eines holoiden Bereichs sind, innerhalb dieses Bereichs niemals mehr als m Wurzeln besitzen kann, es sei denn, daß die Koeffizienten sämtlich verschwinden.

Die Gesamtheit der Wertsysteme, welche man aus

$$(x_{k+1}, x_{k+2}, \ldots, x_m)$$

erhält, wenn man $x_{k+1}, \ldots, x_m$ voneinander unabhängig gleich beliebigen Größen des holoiden Bereichs [A] setzt, ist der einfachste Fall einer dem Bereiche [A] entstammenden $(m-k)$-fachen Mannigfaltigkeit, wo dieser Ausdruck wegen seiner Beziehung auf den beliebigen holoiden Bereich [A] etwas allgemeiner als gewöhnlich verstanden wird; jedes so erhaltene Wertesystem $(\xi_{k+1}, \xi_{k+2}, \ldots, \xi_m)$ sei ein Element der Mannigfaltigkeit $(x_{k+1}, \ldots, x_m)$. Der der Gleichung $D^{(h)} = 0$

zugehörige Komplex von Lösungen ist dann so beschaffen, daß jedem Elemente der Mannigfaltigkeit $(x_{h+2}, \ldots, x_m)$ nur eine endliche Anzahl von Lösungen entspricht, und zwar ist, wenn m_{h+1} den Grad der Gleichung $D^{(h)} = 0$ und $m_h, \ldots, m_1$ die maximalen Grade der Gleichungen $G_1^{(h)} = 0, \ldots, G_h^{(h)} = 0$ in Bezug auf $x_h, x_{h-1}, \ldots, x_1$ angibt*), diese Anzahl niemals größer als $m_1 m_2 \ldots m_h$, kann aber auch 0 sein.

Diese Tatsache wird von besonderer Bedeutung, wenn der vorgelegte holoide Bereich [A] die Eigentümlichkeit darbietet, daß jede innerhalb des Bereichs gebildete Gleichung (mit einer Unbekannten) eine Wurzel besitzt. Ob solche Bereiche existieren, bleibt allerdings jetzt noch dahin gestellt**).

Dann entspricht jedem Elemente der Mannigfaltigkeit

$$(x_{h+2}, \ldots, x_m)$$

in dem zu $D^{(h)} = 0$ gehörigen Komplexe von Lösungen zum mindesten eine, höchstens aber $m_1 \ldots m_{h+1}$ Lösungen, und wir wollen auch dann in Erweiterung der gegebenen Definition diesen Komplex von Lösungen als eine dem Bereiche [A] entstammende $(m-h-1)$-fache Mannigfaltigkeit bezeichnen.

Allerdings können bei dem hier betrachteten ganz allgemeinen Gleichungssysteme (die Anzahl der Gleichungen ist eine beliebige) die sämtlichen $D^{(h)}$ von den Unbestimmten frei sein, und das Gleichungssystem wird dann überhaupt keine Lösungen besitzen, wie dies z. B. schon der einfachste Fall von $n+1$ linearen Gleichungen mit n Unbekannten zeigt. — Insofern Lösungen vorhanden sind, sondern sie sich in $(m-h-1)$-fache Mannigfaltigkeiten, wo h die Werte $0, 1, \ldots, m-1$ an-

---

*) Der Grad der Gleichung $G_1^{(h)} = 0$ kann nicht höher sein als der irgend einer Form $\overline{F}_{j_{h-1}}^{(h-1)}$ und so fort.

**) Es wird sich später zeigen, daß ein solcher holoider Bereich zum mindesten die Gesamtheit der sogenannten „algebraischen Zahlen" umfassen muß. Es ist dies eine unmittelbar einzusehende Folgerung aus der Definition der algebraischen Zahlen in Kap. IV, § 6. Im Gebiete der Analysis ist die Gesamtheit der komplexen Zahlen ein solcher Bereich.

nehmen kann. Die „0-fache“ Mannigfaltigkeit besteht aus einer endlichen Anzahl von Wertsystemen $\xi_1, \ldots, \xi_m$, die Lösungen des vorgelegten Gleichungssystems sind.

Die Discriminante einer Form.

§ 22. Es seien $F = A_0 x^m + \cdots$, $G = B_0 x^n + \cdots$ zwei holoide wirkliche Formen aus $[A, x_1 \ldots x_m, x]$, und G ein Teiler von F. Dabei bezieht sich — um wie früher auch unvollständige holoide Bereiche in die Resultate einzubeziehen — der Begriff der Teilbarkeit auf denjenigen Formenbereich, welcher dem orthoiden Bereiche (A) entstammt. G heißt sodann ein k-facher Teiler von F, wenn F durch G^k noch teilbar, aber nicht mehr durch G^{k+1} teilbar ist. G ist insbesondere ein mehrfacher Teiler, wenn $k > 1$. Dann gilt der Satz:

Die Form F besitzt dann und nur dann einen mehrfachen wirklichen Teiler, wenn der größte gemeinschaftliche Teiler von F und $F' = \frac{\partial F}{\partial x}$ die Unbestimmte x enthält.

Aus $F = G^k H$ folgt unmittelbar $F' = G^k H' + k G^{k-1} H G'$; also ist in der Tat für $k > 1$ sowohl F als F' zum mindesten durch G teilbar.

Besitzen umgekehrt F und F' den größten gemeinschaftlichen Teiler D und enthält D die Unbestimmte x, ist also D' von 0 verschieden, so folgt aus

$$F = DK, \quad F' = DK_1, \quad (K, K_1) \sim 1$$

weiter auch

$$F' = DK' + D'K,$$

und da F' durch D teilbar ist, auch

$$D'K = DK_2.$$

Dann muß aber

$$D_1 = (D, K)$$

x wirklich enthalten. Sonst wäre, wenn man K als Form von x auffaßt, K_2 durch die primitive Form von K teilbar, also D' zum mindesten vom gleichen Grade in x wie D. Nun ist aber D' in x von einem um eine Einheit niedrigeren Grade

als D. Demnach enthält D und K die wirkliche Form D_1 als Teiler, und F ist also zum mindesten durch D_1^2 teilbar. Von der orthoiden Form $D = \frac{\overline{D}_1}{A}$ geht man, wie dies wiederholt auseinandergesetzt wurde, wieder zur holoiden Form $\overline{D}_1$ über, die gleichfalls ein mehrfacher Teiler von F ist.

Wir haben also, um Kriterien für die Existenz eines mehrfachen Teilers zu gewinnen, den größten gemeinschaftlichen Teiler von

$$F = A_0 x^m + A_1 x^{m-1} + \cdots + A_{m-1} x + A_m$$

und

$$\frac{\partial F}{\partial x} = m A_0 x^{m-1} + (m-1) A_1 x^{m-2} + \cdots + A_{m-1}$$

zu untersuchen. Hierzu dient die Resultante der beiden Formen. Diese ist, sobald nur $m > 1$, in der Sylvesterschen Determinante unmittelbar gegeben. Man hat bloß in dieser (§ 14)

$$n = m - 1,\ B_0 = m A_0,\ B_1 = (m-1) A_1,\ \ldots,\ B_{m-1} = A_{m-1}$$

zu setzen. Da dann in der ersten Zeile der Faktor A_0 in Evidenz tritt, kann er vor die Determinante gesetzt werden; die dann auftretende Determinante soll, wenn F von höherem als dem ersten Grade ist, als Discriminante der Form F bezeichnet und mit Dscr. F, nötigenfalls mit Dscr. $\binom{F}{x}$ bezeichnet werden.

Ihre Definition ist demnach in der Relation

$$\text{Res.}\left(F, \frac{\partial F}{\partial x}\right) = A_0 \text{ Dscr. } (F)$$

gegeben, und sie ist ausführlich geschrieben:

$$\begin{vmatrix}
1 & & & & m & & & & \\
A_1 & A_0 & & & (m-1)A_1 & mA_0 & & & \\
\cdot & A_1 & \cdot & & \cdot & (m-1)A_1 & \cdot & & \\
\cdot & \cdot & \cdot & A_0 & \cdot & \cdot & \cdot & mA_0 & \\
\cdot & \cdot & \cdot & & A_{m-1} & \cdot & \cdot & (m-1)A_1 & \\
A_m & \cdot & \cdot & & & A_{m-1} & \cdot & \cdot & \\
 & A_m & \cdot & & & & \cdot & \cdot & \\
 & & \cdot & & & & & A_{m-1} & \\
 & & & A_m & & & & &
\end{vmatrix} \quad (D)$$

Um sogleich eine für das Folgende fundamentale Darstellung dieser Discriminante zu erhalten, bemerke man, daß bei ihrer Entwicklung solche Glieder, die A_0 enthalten, und solche, die A_0 nicht enthalten, unterschieden werden können. Die Summe der Glieder erster Art sei $A_0\Phi$, wo Φ eine rationale und ganze Form der Größen $A_0, \ldots, A_m$ ist. Die Summe der Glieder zweiter Art erhält man unmittelbar, wenn in jener Determinante A_0 gleich Null gesetzt wird. In diesem Falle bleiben aber in der ersten und zweiten Zeile nur die Elemente

$$c_{11} = 1, \quad c_{1m} = m,$$
$$c_{21} = A_1, \quad c_{2m} = (m-1)A_1$$

von 0 verschieden. Es geht also Dscr. F für $A_0 = 0$ in ein Produkt von zwei Faktoren über, von denen der erste $-A_1$ und der zweite

$$(-1)^{m-2} A_1 \,\mathrm{Dscr.}\,(F - A_0 x^m)$$

ist. Setzt man nämlich die m^{te} Spalte zwischen die erste und zweite, wobei die Determinante mit $(-1)^{m-2}$ multipliziert wird, so wird jene Zerlegung evident, und die als zweiter Faktor erscheinende Determinante ist, wie die Anschauung unmittelbar lehrt, die Resultante der Form

$$A_1 x^{m-1} + A_2 x^{m-2} + \cdots + A_m = F - A_0 x^m$$

und ihrer Derivierten nach x. Man hat also für die Discriminante die fundamentale Identität

$$\mathrm{Dscr.}\,(F) = A_0\Phi + (-1)^{m-1} A_1^2 \,\mathrm{Dscr.}\,(F - A_0 x^m) \quad (\mathrm{D}_1)$$

gewonnen, wo der Grad von F größer als eins vorausgesetzt ist.

Die Discriminante der Form zweiten Grades ist

$$4A_0A_2 - A_1^2.$$

§ 23. Man erhält — in Analogie mit den für die Resultante gültigen Entwicklungen — zwei fundamentale Eigenschaften der Discriminante, deren erste in folgendem Satze enthalten ist:

Die Discriminante einer Form $F(x)$ verschwindet dann und nur dann, wenn die Form einen solchen mehrfachen Teiler besitzt, der x wirklich enthält, oder aber die Koeffizienten A_0 und A_1 beide gleich 0 sind.

Dabei ist — insofern der zu Grunde liegende Bereich [A] kein vollständiger holoider Bereich wäre — die Teilbarkeit in dem aus dem orthoiden Bereiche (A) entstammenden Formenbereiche zu verstehen.

Ist A_0 von 0 verschieden, so wird die Resultante der Formen F und $\frac{\partial F}{\partial x}$ dann und nur dann verschwinden, wenn die Discriminante von F verschwindet, und der angegebene Satz ist also für $A_0 \neq 0$ jedenfalls richtig. Ist aber $A_0 = 0$ und auch $A_1 = 0$, so ist nach (D_1) auch $\Delta = \text{Dscr.}(F) = 0$. — Ist umgekehrt $A_0 = 0$ und auch $\Delta = 0$, so muß entweder $A_1 = 0$ sein, oder aber die Discriminante der Form

$$F - A_0 x^m = A_1 x^{m-1} + \cdots + A_m,$$

die jetzt, da $A_0 = 0$, mit F übereinstimmt, verschwinden; und diese hat, wenn eben $A_1 \neq 0$ ist, in der Tat einen mehrfachen Teiler.

Der zweite Fundamentalsatz lautet:

Die Discriminante Δ der Form $F(x)$, die von höherem als dem ersten Grade vorausgesetzt ist, genügt einer Identität

$$\Delta = GF + G_1 \frac{\partial F}{\partial x},$$

wo G und G_1 zwei Formen von x bedeuten, deren Koeffizienten rationale und ganze Formen der ursprünglichen Koeffizienten $A_0, A_1, \ldots, A_m$ sind.

Der Beweis dieses Satzes wird uns das erste Beispiel für die Anwendung einer in ähnlichen Fällen durchweg anwendbaren und daher sehr weittragenden Methode liefern.

Für $\text{Res.}\left(F, \frac{\partial F}{\partial x}\right) = A_0 \Delta$ existiert nach § 16 jedenfalls eine ähnliche Identität. Sie lautet, wenn F' für $\frac{\partial F}{\partial x}$ geschrieben wird:

$$A_0 \Delta = HF + H_1 F'.$$

Diese Identität ist für jedes Koeffizientensystem gültig, also auch dann, wenn für A_m die Größe $A_m - F(u)$ gesetzt wird*). Dabei ändern sich A_0 und F' überhaupt nicht, während $F(x)$ in $F(x) - F(u)$ übergeht. Aus Δ, H und H' mögen dann die Formen $\Delta^{(u)}$, $H^{(u)}$ und $H_1^{(u)}$ entstehen. Man hat demnach:

$$A_0 \Delta^{(u)} = H^{(u)}(F(x) - F(u)) + H_1^{(u)} F'$$

oder also, da $F(x) - F(u)$ durch $x - u$ teilbar ist,

$$A_0 \Delta^{(u)} \equiv H_1^{(u)} F' \pmod{x - u}.$$

Entwickelt man daher

$$F'(x) = F'(u + x - u) = F'(u) + \cdots, \quad H_1^{(u)} = H_2^{(u)} + \cdots$$

nach Potenzen von $x - u$, so ist

$$A_0 \Delta^{(u)} - H_2^{(u)} F'(u) \equiv 0 \pmod{x - u}.$$

Da aber die linke Seite x überhaupt nicht enthält und doch durch $x - u$ teilbar ist, muß sie gleich 0 sein. Nun ist u das Zeichen einer neuen Unbestimmten. Man kann dafür jetzt wieder x setzen und hat demnach

$$A_0 \Delta^{(x)} = H_2^{(x)} F'(x).$$

Diese Identität bleibt auch dann richtig, wenn man die $A_0, A_1, \ldots, A_m$ als Unbestimmte auffaßt. In dieser Auffassung ist aber

$$F'(x) = m A_0 x^{m-1} + (m-1) A_1 x^{m-2} + \cdots + A_{m-1}$$

eine primitive Form von x, deren Koeffizienten dem Bereiche $[[1], A_0, A_1, \ldots]$ angehören. Mit $A_0 \Delta^{(x)}$ muß also auch schon $\Delta^{(x)}$ durch $F'(x)$ teilbar sein; und es wird

$$\Delta^{(x)} = G_1 F'(x),$$

wo G_1 eine rationale und ganze Form von $A_0, \ldots, A_m, x$ ist.

*) Diese wichtige Substitution wurde zuerst von Kronecker für die Resultante angewendet (Festschrift, § 20).

Andrerseits entsteht $\Delta^{(x)}$ aus Δ, wenn man für A_m die Größe $A_m - F(x)$ setzt. Entwickelt man demnach $\Delta^{(x)}$ nach Potenzen von $F(x)$, so wird

$$\Delta^{(x)} = \Delta - GF$$

und demnach, wie zu beweisen war,

$$\Delta = GF + G_1 F',$$

eine Identität, die richtig ist, wenn die A unbestimmte Größen sind, also auch dann gültig sein muß, wenn die Größen A irgend welche Größen des Bereichs [A] sind.

Resultante und Discriminante als symmetrische Form.

§ 24. Setzt man, wie dies schon in Kap. II, § 11 geschah:

$$\begin{aligned} P(z) &= (z - x_1)(z - x_2) \ldots (z - x_m) \\ &= z^m - \mathfrak{f}_1 z^{m-1} + \mathfrak{f}_2 z^{m-2} - \cdots + (-1)^m \mathfrak{f}_m, \end{aligned}$$

wo $\mathfrak{f}_1, \ldots, \mathfrak{f}_m$ die elementaren symmetrischen Formen von $x_1, \ldots, x_m$ bedeuten, und ähnlich noch

$$\begin{aligned} Q(z) &= (z - y_1)(z - y_2) \cdots (z - y_n) \\ &= z^n - \mathfrak{g}_1 z^{n-1} + \mathfrak{g}_2 z^{n-2} - \cdots + (-1)^n \mathfrak{g}_n, \end{aligned}$$

wo $\mathfrak{g}_1, \ldots, \mathfrak{g}_n$ wieder die elementaren symmetrischen Formen der Unbestimmten $y_1, \ldots, y_n$ sind, so sollen nun die Formen

$$\overline{F}(z) = A_0 P(z), \quad \overline{G}(z) = B_0 Q(z)$$

betrachtet werden.

Die Resultante dieser beiden Formen kann nach § 14 dieses Kapitels als Determinante direkt hingeschrieben werden, und zwar wird, wenn man die in den einzelnen Spalten auftretenden Faktoren A_0 und B_0 vor die Determinante setzt:

$$\text{Res.}(\overline{F}, \overline{G}) =$$

$$A_0^n B_0^m \begin{vmatrix} 1 & & & & 1 & & & \\ -\mathfrak{f}_1 & \cdot & & & -\mathfrak{g}_1 & \cdot & & \\ \mathfrak{f}_2 & \cdot & \cdot & & \mathfrak{g}_2 & \cdot & \cdot & \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & -\mathfrak{f}_1 & \cdot & \cdot & \cdot & -\mathfrak{g}_1 \\ \cdot & \cdot & \cdot & \mathfrak{f}_2 & \cdot & \cdot & \cdot & \mathfrak{g}_2 \\ (-1)^m \mathfrak{f}_m & \cdot & \cdot & \cdot & (-1)^n \mathfrak{g}_n & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot \\ & & \cdot & \cdot & & & \cdot & \cdot \\ & & & (-1)^m \mathfrak{f}_m & & & & (-1)^n \mathfrak{g}_n \end{vmatrix}.$$

Multipliziert man die erste Zeile dieser Determinante mit x_k^{m+n-1}, allgemein die i^{te} Zeile mit x_k^{m+n-i}, und addiert die so erhaltenen Zeilen zur letzten Zeile, so erhält man für $\frac{\text{Res.}(\overline{F}, \overline{G})}{A_0^n B_0^m}$ eine Determinante Γ, deren letzte Zeile aus den folgenden Elementen besteht. Es ist

$$c_{m+n,\,j} = x_k^{n-j} P(x_k) = 0 \qquad (j = 1, 2, \ldots, n)$$
$$c_{m,\,n+j'} = x_k^{n-j'} Q(x_k) \qquad (j' = 1, 2, \ldots, m).$$

In der Formel

$$\text{Res.}(\overline{F}, \overline{G}) = A_0^n B_0^m \Gamma$$

ist die Determinante Γ jedenfalls eine rationale und ganze Form der Elemente x und y und nach der Bestimmung der in der letzten Zeile stehenden Elemente durch

$$Q(x_k) = (x_k - y_1)(x_k - y_2) \cdots (x_k - y_n)$$

teilbar.

Nun ist der größte gemeinschaftliche Teiler von $Q(x_k)$ und $Q(x_i)$ gleich Eins. Denn er kann weder x_k noch x_i enthalten, muß mithin Teiler des Koeffizienten jeder Potenz von x_k in $Q(x_k)$ sein, also schließlich, da der Koeffizient von x_k^n die Einheit ist, gleich eins sein. Demnach wird $\frac{\text{Res.}(\overline{F}, \overline{G})}{A_0^n B_0^m}$ auch durch $\prod_{k=1}^{m} Q(x_k)$ teilbar sein, und man hat

$$\text{Res.}(\overline{F}, \overline{G}) = C A_0^n B_0^m \prod_{k=1}^{m} Q(x_k).$$

Dabei erkennt man leicht, daß $C = 1$. Denn für den ursprünglichen Ausdruck von Res. $(\overline{F}, \overline{G})$ wird jenes Glied, das in den Unbestimmten y die höchste Dimension besitzt, unmittelbar $(-1)^{mn} A_0^n B_0^m \mathfrak{g}_n^m = (-1)^{mn} A_0^n B_0^m (y_1 \cdots y_n)^m$, während in dem jetzt erhaltenen Ausdruck, wenn man den Wert von $Q(x_k)$ in Betracht zieht, die Glieder höchster Dimension jedenfalls in

$$C A_0^n B_0^m (-1)^{mn} (y_1 \cdots y_n)^m$$

enthalten sind. Es muß also C von den x frei sein und mit jenem Gliede höchster Dimension übereinstimmen, was in der Tat $C = 1$ ergibt.

Dieses Resultat lautet auch:

$$\text{Res.}\,(\overline{F}, \overline{G}) = A_0^n B_0^m \prod (x_k - y_l). \qquad \begin{pmatrix} k = 1, \ldots, m \\ l = 1, \ldots, n \end{pmatrix}$$

Der links stehende Ausdruck ist daher eine Form der elementaren symmetrischen Formen der x und auch der y und durch diese Identität vollständig bestimmt; denn zwei Formen der $\mathfrak{f}$ und $\mathfrak{g}$, deren jede gleich dem rechts stehenden Produkte, sind unbedingt identisch. Es müssen nämlich nach Kap. II, § 14 zuerst die Koeffizienten irgend eines Potenzproduktes der $\mathfrak{f}$ auf beiden Seiten dieselben sein; diese Koeffizienten sind aber rationale und ganze Formen der $\mathfrak{g}$, und nach demselben Satze müssen auch in diesen Formen die einzelnen Koeffizienten dieselben sein.

Man kann also auch

$$\mathfrak{f}_i = \frac{(-1)^i A_i}{A_0}, \quad \mathfrak{g}_j = \frac{(-1)^j B_j}{B_0}$$

setzen; dabei gehn aber die Formen $\overline{F}(z)$ und die $\overline{G}(z)$ in die „allgemeinen“ Formen

$$F(z) = A_0 z^m + A_1 z^{m-1} + \cdots + A_m$$
$$G(z) = B_0 z^n + B_1 z^{n-1} + \cdots + B_n,$$

ferner Res. $(\overline{F}, \overline{G})$ in Res. (F, G) über; man erhält so die folgende wichtige „symbolische“ Darstellung der Resultante zweier Formen:

$$\text{Res.}\,(F, G) = A_0^n B_0^m \prod (x_k - y_l). \qquad \begin{pmatrix} k = 1, \ldots, m \\ l = 1, \ldots, n \end{pmatrix} \quad (\mathrm{R}_1)$$

Diese Bestimmung ist so zu verstehn, daß die rechts stehende Form zuerst als Form der elementaren symmetrischen Formen $\mathfrak{f}$ und $\mathfrak{g}$ darzustellen ist und dann statt dieser:

$$\mathfrak{f}_i = \frac{(-1)^i A_i}{A_0}, \quad \mathfrak{g}_j = \frac{(-1)^j B_j}{B_0}$$

gesetzt werden muß.

Vertauscht man die Rolle der beiden Formen F und G, so wird ebenso:

$$\begin{aligned}\text{Res.}(G, F) &= A_0^n B_0^m \prod (y_l - x_k) \\ &= (-1)^{mn} A_0^n B_0^m \prod (x_k - y_l),\end{aligned}$$

also wieder

$$\text{Res.}(F, G) = (-1)^{mn} \text{Res.}(G, F).$$

Schließlich kann man noch die Werte von $\mathfrak{g}_j$ schon in die Teilprodukte

$$\begin{aligned}&B_0(x_k - y_1)(x_k - y_2) \cdots (x_k - y_l) \\ &= B_0(x_k^n - \mathfrak{g}_1 x^{n-1} + \cdots + (-1)^n \mathfrak{g}_n)\end{aligned}$$

einsetzen und erhält dann für die Resultante die — ebenso wie oben — zu interpretierende zweite symbolische Form

$$\text{Res.}(F, G) = A_0^n \prod_{k=1}^{m} G(x_k) \qquad (\mathrm{R}_2)$$

und ebenso

$$\text{Res.}(G, F) = B_0^m \prod_{l=1}^{n} F(y_l)$$

oder also auch

$$\text{Res.}(F, G) = (-1)^{mn} B_0^m \prod_{l=1}^{n} F(y_l). \qquad (\mathrm{R}_3)$$

§ 25. Um eine ähnliche Darstellung der Discriminante zu finden, haben wir nur zu berücksichtigen, daß diese aus der Resultante von $F(z)$ und $F'(z)$ durch Entfernung des Faktors A_0 entsteht; man hat also unmittelbar aus (R_2)

$$\text{Dscr. } F = A_0^{m-2} \prod_{k=1}^{m} F'(x_k). \qquad (\Delta_2)$$

Wendet man (Δ_2) jetzt auf die Form

$$\overline{F}(z) = A_0 P(z) = A_0(z^m - \mathfrak{f}_1 z^{m-1} + \cdots + (-1)^m \mathfrak{f}_m)$$

an, so wird wegen

$$P'(x_k) = (x_k - x_1) \cdots (x_k - x_{k-1})(x_k - x_{k+1}) \cdots (x_k - x_m)$$

weiter:

$$\text{Dscr. } \overline{F} = A_0^{2m-2} \prod_{k=1}^{m} P'(x_k) \qquad \binom{r, s = 1, \ldots, m}{r < s}.$$

$$= (-1)^{\frac{m(m-1)}{2}} A_0^{2m-2} \prod_{r,s} (x_r - x_s)^2$$

Wenn man hierin unter Dscr. $\overline{F}$ den für diese Größe gegebenen Determinanten-Ausdruck versteht, ist nun genau dieselbe Schlußweise gestattet, die zur Darstellung der Resultante in (R_1) führte, und es wird demgemäß

$$\text{Dscr. } F = (-1)^{\frac{m(m-1)}{2}} A_0^{2m-2} \prod_{r,s} (x_r - x_s)^2 \quad \binom{r,s=1,\ldots,m}{r<s}, \quad (\Delta_1)$$

welche Bestimmung genau so wie früher (R_1) zu interpretieren ist, oder auch noch nach Kap. II, § 11

$$\text{Dscr. } F = (-1)^{\frac{m(m-1)}{2}} A_0^{2m-2} [x_1^{m-1}]^2$$

$$= (-1)^{\frac{m(m-1)}{2}} A_0^{2m-2} \Delta(x_1, x_2, \ldots, x_m). \quad (\Delta_1')$$

Viertes Kapitel.

Die algebraischen Größen.

Faktorenzerlegung der rationalen und ganzen Formen.

§ 1. Im Bereiche der rationalen und ganzen Zahlen [1] bestehen vor allem diejenigen Teilbarkeitsgesetze, die überhaupt für vollständige holoide Bereiche gültig sind; darüber hinaus lehren aber die Elemente der Arithmetik zwei weitere fundamentale Sätze, die hier einfach angeführt werden sollen:

I. Jede rationale und ganze Zahl mit Ausnahme der 0 besitzt nur eine endliche Anzahl ebensolcher Teiler, die in einer endlichen Versuchsreihe bestimmt werden können.

II. Jede rationale und ganze Zahl mit Ausnahme von 0, ± 1 ist als Produkt von Primzahlen darstellbar, und zwar ist diese Darstellung im Sinne der Äquivalenz eindeutig bestimmt.

In Bezug auf den zweiten Satz sei noch bemerkt, daß zwei rationale und ganze Zahlen k und k' dann und nur dann äquivalent sind, wenn $k' = \pm k$. Die genauere Formulierung des Satzes ist daher folgende: Ist $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ und auch $n = q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}$, wo $p_1, p_2, \dots, q_1, q_2, \dots$ Primzahlen, so muß $r = s$ sein und weiter $p_1 \sim q_{i_1}$, $p_2 = q_{i_2}, \dots, p_r \sim q_{i_r}$, wo $i_1, i_2, \dots, i_r$ die Zahlen $1, \dots, r$ in einer bestimmten Reihenfolge bedeuten. Selbstverständlich ist mit p auch $-p$ als Primzahl anzusehen. Es ist dann auch $a_1 = b_{i_1}$ u. s. f.

Im Bereiche der rationalen und ganzen Formen $[[1], x_1, \dots x_m]$ bestehen genau die analogen Sätze. Zunächst:

Jede rationale und ganze Form besitzt nur eine endliche Anzahl ebensolcher Teiler, die in einer endlichen Versuchsreihe bestimmt werden können.

Es seien

$$F = \sum_{(g)} k_g x_1^{g_1} \dots x_m^{g_m}, \qquad F_1 = \sum_{(g')} k'_{g'} x_1^{g'_1} \dots x_m^{g'_m},$$

$$F_2 = \sum_{(g'')} k''_{g''} x_1^{g''_1} \dots x_m^{g''_m}$$

solche Formen und

$$F = F_1 F_2.$$

Ist F von der n^{ten} Dimension, so kann der Teiler F_1 nicht von höherer Dimension sein, und man hat daher der Reihe nach jene Teiler zu bestimmen, deren Dimension $0, 1, \dots, n$ ist. Ist dabei F_1 von der k^{ten}, so ist F_2 von der $(n-k)^{\text{ten}}$ Dimension. Es genügt also jene Teiler zu bestimmen, deren Dimension $\frac{n}{2}$ nicht übersteigt, und dabei $n > 0$ anzunehmen. Denn eine Form 0ter Dimension ist eine rationale und ganze Zahl; und ihre Teiler ebensolche Zahlen, deren Reihe unmittelbar angeschrieben werden kann.

Die Teiler 0ter Dimension von F, wo F jetzt eine wirkliche Form bedeutet, sind rationale und ganze Zahlen, die als Teiler im größten gemeinschaftlichen Teiler der Koeffizienten k_g enthalten sind, also wieder in endlicher Anzahl vorhanden und bekannt.

Um die Teiler l^{ter} Dimension zu bestimmen, schreibt man

$$F_1 = \sum_{(g')} k'_{g'} x_1^{g'_1} \dots x_m^{g'_m} \qquad F_2 = \sum_{(g'')} k''_{g''} x_1^{g''_1} \dots x_m^{g''_m}$$

als „allgemeine“ Formen von $x_1, \dots, x_m$ der angegebenen Dimension, d. h. man setze für $g_1, \dots, g_m$ in der ersten Form alle rationalen und ganzen Wertsysteme, für welche $g'_1 + \dots + g'_m \leqq l$, und ebenso in der zweiten Form für $g''_1, \dots, g''_m$ alle jene Wertesysteme, für welche $g''_1 + \dots + g''_m \leqq n-l$, und betrachte die Koeffizienten k'_g, k''_g als unbekannte, d. h. zu bestimmende Größen.

Soll nun $F = F_1 F_2$ sein, so muß nach der Formulierung (K) des Kroneckerschen Fundamentalsatzes in Kap. III § 7 jedes Koeffizientenprodukt $k'_g, k''_{g''}$ einer Identität genügen, die, wenn wir kurz $z = k'_g, k''_{g''}$ setzen, die folgende ist:

$$z^\nu + h_1 z^{\nu-1} + \cdots + h_\nu = 0,$$

wo $h_1, \ldots, h_\nu$ bekannte rationale und ganze Formen der Koeffizienten von $F_1 F_2 = F$, also bekannte rationale und ganze Zahlen sind. Dann muß aber $k'_{g'}$ und auch $k''_{g''}$ ein Teiler des letzten nicht verschwindenden Koeffizienten h sein; oder aber es ist, wenn $h_\nu = 0$, eine der Größen $k'_{g'}, k''_{g''}$ gleich Null. Da nun aber weder die sämtlichen k' noch die sämtlichen k'' verschwinden, erhält man für jede dieser Größen bei Benutzung der Gleichungen für alle Produkte $k'_{g'} k''_{g''}$ jedenfalls eine endliche Reihe bestimmter Werte. Dasselbe ist dann aber auch für die Formen F_1, F_2 der Fall. Ob eine so bestimmte Form F_1 auch wirklich eine Relation $F = F_1 F_2$ zur Folge hat, bleibt dabei noch zweifelhaft, wird aber in jedem einzelnen Falle einfach durch Division entschieden; so daß unserem Satze gemäß die volle Reihe der Teiler von F in einer endlichen Anzahl von Schritten erlangt wird. Dabei sind wieder F_1 und $-F_1$ und nur diese als im Sinne der Aquivalenz nicht verschieden anzusehen*).

§ 2. Da $[[1], x_1, \ldots, x_m]$ ein vollständiger holoider Bereich ist, fällt in ihm der Begriff der irreduziblen Größe und der Primgröße zusammen. Diese sollen nun als (rationale und ganze) Primformen, Primteiler bezeichnet werden und sind

*) Eine andere Methode zur Bestimmung der Teiler von F, die von der Lagrangeschen Interpolationsformel ausgeht, hat Kronecker angegeben („Festschrift", § 4). Die Ausführungen im Texte sind prinzipiell einfacher, weil sie die Werte der ganzen Funktion F nicht benutzen, also ausschließlich in der Theorie der Formen bleiben. Ein Verfahren zur Abkürzung der äußerst langwierigen Rechnung hat Runge angegeben (Journ. f. Math., Bd. 99, pag. 89). Zur Anfertigung von Tabellen leitet die obige Anwendung des Fundamentalsatzes, insofern für Formen einer bestimmten Dimension die Formen h dieselben bleiben.

also entweder Primzahlen oder wirkliche Primformen und dann jedenfalls auch primitiv.

Jede von ± 1 verschiedene Form hat nun zum mindesten einen Primteiler. Sind die (im Sinne der Äquivalenz) verschiedenen Teiler von F bloß 1 und F, so ist F selbst eine Primform. Im entgegengesetzten Falle hat F einen von 1 und F verschiedenen Teiler G, also ist G nicht durch F teilbar. Sämtliche Teiler von G sind aber auch Teiler von F. Die Anzahl der Teiler von G ist also kleiner als die Anzahl der Teiler von F. Nun ist wieder G entweder eine Primform oder durch eine von 1 und G verschiedene Form G_1 teilbar. Die Fortsetzung dieses Verfahrens führt somit zu einer Reihe von Formen

$$F, G, G_1, \ldots, G_s;$$

das Verfahren muß aber notwendigerweise abbrechen, da die Anzahl der Teiler immer kleiner wird. Es muß also nach $s+1$ Schritten G_s eine Primform sein.

Ist nun F durch die Primform P_1 teilbar, so wird entweder $F = \pm P_1$, d. h. $F \sim P_1$; oder aber $F = P_1 F_1$ und F_1 wieder durch eine Primform P_2 teilbar; also $F_1 = P_2 F_2$ u. s. f. Man erhält also schließlich:

$$F \sim P_1 P_2 \ldots P_r,$$

wo das Verfahren wieder abbricht, d. h. r eine bestimmte positive ganze Zahl ist, denn die Anzahl der Teiler von F_1, F_2, ... wird immer kleiner; es wird also schließlich $F_r \sim 1$. Wäre nun auch

$$F \sim Q_1 Q_2 \ldots Q_s,$$

wo $Q_1, Q_2, \ldots$ wieder Primformen bedeuten, so muß

$$F \sim Q_1 Q_2 \ldots Q_s$$

durch P_1 teilbar sein; also ist entweder Q_1 oder $Q_2 \ldots Q_s$ durch P_1 teilbar. Ist das erste nicht der Fall, so muß $Q_2 \ldots Q_s$, also auch Q_2 oder $Q_3 \ldots Q_s$ durch P_1 teilbar sein und so fort; es ist also jedenfalls eine Primform Q_{i_1} durch P_1 teilbar;

nun hat aber Q_{i_1} als irreduzible Größe nur die zwei verschiedenen Teiler 1 und Q_{i_1}, es muß also

$$P_1 \sim Q_{i_1}$$

sein; ebenso $P_2 \sim Q_{i_2}$ und so fort, also auch $r = s$. Damit ist der Hauptsatz für die Faktorenzerlegung im rationalen und ganzen Formenbereiche gewonnen:

Jede rationale und ganze Form mit Ausnahme von 0 und ± 1 ist als Produkt ebensolcher Primteiler darstellbar, und zwar ist diese Darstellung im Sinne der Äquivalenz eindeutig bestimmt.

Da äquivalente Formen sich nur im Vorzeichen unterscheiden können, folgt in dem betrachteten Bereiche aus diesem Satze auch der früher bewiesene von der endlichen Anzahl der Teiler. Faßt man die eventuell mehrfach vorkommenden Primteiler zusammen, so wird die Darstellung von F die folgende

$$F \sim P_1^{a_1} P_2^{a_2} \dots P_h^{a_h},$$

und man sieht, daß jeder Teiler von F in der Gestalt

$$G \sim P_1^{b_1} P_2^{b_2} \dots P_h^{b_h} \qquad (b_i \leqq a_i)$$

darstellbar sein muß.

Faktorenzerlegung in orthoiden Formenbereichen.

§ 3. Geht man von einem orthoiden Bereiche (A) aus und betrachtet den ihm enstammenden Formenbereich $[(A), x_1, \dots, x_m]$, so sind in diesem die Formen AF und BF äquivalent, wenn A und B zwei von 0 verschiedene Größen aus (A) sind; denn es ist in diesem Falle den schon öfter besprochenen Äquivalenzbestimmungen gemäß $A \sim 1$ und $B \sim 1$.

In einem solchen Bereiche sind demnach alle wirklichen linearen Formen Primformen. Eine lineare Form L kann keinesfalls durch Formen höherer Dimension teilbar sein. Jeder Teiler ist also entweder eine von 0 verschiedene Größe aus (A) und demnach ~ 1, oder aber eine lineare Form

L_1. Dann muß aber in $L = AL_1$ die Größe A dem Bereiche (A) angehören und nicht 0 sein, mithin ist $A \sim 1$ und $L_1 \sim L$.

Ferner ist allgemeiner, wenn G ein Teiler der von 0 verschiedenen Form F und G von derselben Dimension wie F ist, immer $F \sim G$. Denn in $F = AG$ muß dann A dem Bereiche (A) angehören, also $A \sim 1$ sein.

Ist nun die Form F nicht selbst schon eine Primform und auch keine Größe des Bereichs (A) (also weder 0 noch ~ 1), so muß sie echte Teiler besitzen, deren Dimension kleiner als die Dimension von F und zumindest gleich 1 ist. Unter diesen gibt es jedenfalls eine Form P_1 kleinster Dimension. Diese muß eine Primform sein. Denn ein Teiler derselben ist jedenfalls auch ein Teiler von F. Wäre dieser aber ein echter Teiler von P_1, so müßte er auch von kleinerer Dimension als P_1 sein, was der Annahme widerspricht.

Ist nun $F = P_1 F_1$, so ist F_1 von kleinerer Dimension als F. Man erhält dann wieder $F_1 = P_2 F_2$ und so fort. Dieses Verfahren muß aber nach einer endlichen Anzahl von Schritten abbrechen; wenn nicht früher, so doch dann, wenn man zu einer linearen Form gelangt; und dies geschieht im ungünstigsten Falle nach $n - 1$ Schritten, wenn n die Dimension von F bedeutet.

Man hat daher wieder den Satz:

Jede wirkliche orthoide Form ist als Produkt ebensolcher Primformen darstellbar, und zwar ist diese Darstellung im Sinne der Äquivalenz eindeutig bestimmt.

Denn aus $F \sim P_1 \dots P_r$ und $F \sim Q_1 \dots Q_s$ folgt genau wie früher $r = s$, $P_1 \sim Q_{i_1}, \dots$, da der betrachtete Formenbereich wieder ein vollständiger Bereich ist.

Demnach hat — in wörtlicher Wiederholung der früheren Schlüsse — jede von 0 verschiedene Form nur eine endliche Anzahl nicht äquivalenter Teiler.

Dabei soll aber sogleich auf eine sehr wesentliche Lücke in dem befolgten Gedankengange hingewiesen werden. Der Satz gibt nur einen s. g. Existenzbeweis, und es fehlt jede

Vorschrift, um die Darstellung einer Form als Produkt von Primformen wirklich zu erhalten. Beim Mangel einer jeden weiteren Bestimmung des Bereichs (A) ist das auch unmöglich.

Der aus (A) entstammende Formenbereich ist demnach nur dann als wohldefiniert zu betrachten, wenn eine Vorschrift vorhanden ist, die in einer endlichen Anzahl von Schritten zu jeder von 0 verschiedenen Form eine Primform ergibt, durch welche sie teilbar ist. Daß damit die Darstellung als Produkt von Primformen geliefert ist und auch die Reihe der nicht äquivalenten Teiler von F aufgestellt werden kann, ist klar.

Wir erhalten nun wieder eine feste Grundlage für unsere weiteren Untersuchungen durch den Satz, daß jede von 0 verschiedene rationale Form in einer endlichen Anzahl von Operationen als Produkt von ebensolchen Primformen dargestellt werden kann.

Dazu ist nur zu bemerken, daß jede rationale Form in der Gestalt

$$\sum_{(g)} \frac{k_g}{l} x_1^{g_1} \dots x_m^{g_m} = \frac{k}{l} \sum_{(g)} k'_g x_1^{g_1} \dots x_m^{g_m}$$

geschrieben werden kann, wo k den größten gemeinschaftlichen Teiler der rationalen ganzen Zahlen k_g bedeutet und demnach

$$(\dots, k'_g, \dots) \sim 1$$

wird. Jede rationale Form ist demnach das Produkt einer rationalen Zahl und einer rationalen und ganzen primitiven Form oder also dieser letzteren äquivalent. Wird sie mit X bezeichnet und ist

$$X \sim P_1 P_2 \dots P_r$$

im Sinne der für rationale und ganze Formen gegebenen Zerlegung in Primformen, so ist auch im rationalen Formenbereiche

$$F \sim P_1 P_2 \dots P_r$$

eine Zerlegung in Primformen. Denn es ist nun $F \sim X$, ferner jedes P auch eine wirkliche Form, denn X ist als

primitive Form durch keine Primzahl teilbar, und es ist endlich P auch im rationalen Formenbereiche irreduzibel. Wäre nämlich P das Produkt zweier wirklicher Formen, so ließen sich diese jedenfalls wieder $\frac{k_1}{l_1} X_1$ und $\frac{k_2}{l_2} X_2$ schreiben, wo k_1, l_1, k_2, l_2 ganze Zahlen, X_1, X_2 rationale und ganze primitive Formen sind. Also wäre

$$l_1 l_2 P = k_1 k_2 X_1 X_2,$$

ferner, da auch $X_1 X_2$ primitiv ist, $k_1 k_2 = \pm l_1 l_2$ und

$$P = \pm X_1 X_2,$$

also P im Widerspruche zur Annahme auch im rationalen und ganzen Formenbereiche zerlegbar.

Für Formen mit einer Unbestimmten z, sowie für reguläre Formen überhaupt sei noch insbesondere bemerkt, daß man unter den äquivalenten Formen immer diejenige wählen kann, in welcher der Koeffizient der höchsten Potenz von z Eins ist. Hat man dann irgend eine Zerlegung

$$F \sim F_1 F_2 \dots F_s$$

und setzt für

$$F = A_0 z^m + A_1 z^{m-1} + \cdots$$

$$\overline{F} = z^m + \frac{A_1}{A_0} z^{m-1} + \cdots$$

und in ähnlicher Weise $\overline{F}_1, \dots, \overline{F}_s$ für $F_1, F_2, \dots, F_s$ so wird

$$\overline{F} = \overline{F}_1 \overline{F}_2 \dots \overline{F}_s;$$

denn es ist jedenfalls

$$\overline{F} = C \overline{F}_1 \overline{F}_2 \dots \overline{F}_s,$$

und die Vergleichung der Koeffizienten ergibt unmittelbar $C = 1$.

§ 4. Der im vorstehenden für P bewiesene Satz läßt sich folgendermaßen aussprechen:

Ist P irreduzibel im Bereiche der rationalen und ganzen Formen, so ist P auch im Bereiche der rationalen Formen irreduzibel.

Dem für wirkliche Formen schon bewiesenen Satze ist

nur der Fall hinzuzufügen, wo P eine Primzahl ist; der Satz ist auch dann gültig, weil im rationalen Formenbereiche $P \sim 1$ wird.

Daraus können wir nun unmittelbar folgern, daß es sowohl im rationalen wie im rationalen und ganzen Formenbereiche unendlich viele Primformen von beliebig gegebener Dimension gibt.

Nach einem von Eisenstein*) herrührenden Satze ist nämlich die Form

$$z^m + c_1 z^{m-1} + \cdots + c_{m-1} z + c_m,$$

wo $c_1, \ldots, c_{m-1}$ durch eine gewisse Primzahl p teilbare ganze Zahlen sind und c_m wohl durch p, aber nicht durch p^2 teilbar ist, immer irreduzibel im Bereiche der rationalen und ganzen, also auch der rationalen Formen.

Wäre das Gegenteil der Fall, so müßte jene Form als Produkt

$$(z^g + k_1 z^{g-1} + \cdots + k_g)\,(z^{m-g} + k'_1 z^{m-g-1} + \cdots + k'_{m-g})$$

geschrieben werden können. Man erhält durch Vergleichung der Koeffizienten, wenn k'_j für $j < 0$ die Bedeutung 0 erhält und $k'_0 = 1$ gesetzt wird:

$$\begin{aligned}
k_g k'_{m-g} &= c_m \\
k_{g-1} k'_{m-g} + k_g k'_{m-g-1} &= c_{m-1} \\
\cdots\cdots\cdots\cdots & \\
k_1 k'_{m-g} + k_2 k'_{m-g-1} + \cdots + k_g k'_{m-2g+1} &= c_{m-g+1} \\
k'_{m-g} + k_1 k'_{m-g-1} + \cdots + k_{g-1} k'_{m-2g+1} + k_g k'_{m-2g} &= c_{m-g}.
\end{aligned}$$

Nun ist, da c_m wohl durch p, nicht aber durch p^2 teilbar ist, eine und nur eine der Zahlen k_g, k'_{m-g} durch p teilbar. Ohne Beeinträchtigung der Allgemeinheit kann vorausgesetzt werden, daß z. B. k_g die durch p teilbare Zahl ist; im entgegengesetzten Falle hat man nur die beiden Faktoren zu vertauschen. Dann

*) Journ. f. Math., Bd. 59, pag. 160.

muß aber, weil in der zweiten Gleichung c_{m-1}, sowie k_g durch p teilbar und k'_{m-g} nicht teilbar ist, auch k_{g-1} durch p teilbar sein. Ebenso aus der dritten Gleichung $k_{g-2}, \ldots$ und so fort bis k_1. Dann wäre aber nach der letzten Gleichung im Widerspruche zur Annahme für die untersuchte Form auch k'_{m-g} durch p und c_m durch p^2 teilbar; womit der Satz bewiesen ist.

Als einfaches Corollar dieses Satzes sei noch hier seiner vielfachen Anwendung wegen der folgende erwähnt:

Für jede Primzahl p ist die Form

$$z^{p-1} + z^{p-2} + \cdots + z + 1$$

im rationalen, sowie im rationalen und ganzen Formenbereiche irreduzibel.

Die Form bleibt reduzibel oder irreduzibel, wenn man die Transformation $z = y + 1$ anwendet. Dann ist aber wegen

$$(z - 1)(z^{p-1} + \cdots + 1) = z^p - 1$$

auch

$$y((y+1)^{p-1} + \cdots + 1) = (y+1)^p - 1 =$$
$$= y^p + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots + \binom{p}{1} y;$$

und also

$$(y+1)^{p-1} + \cdots + 1 = y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{2} y + \binom{p}{1}$$

dem Eisensteinschen Satze gemäß eine irreduzible Form.

Neue Fassung des Gleichungsproblems. Die Adjunktion.

§ 5. Als dem orthoiden Bereiche (A) entstammende Gleichung n^{ten} Grades mit einer Unbekannten bezeichnen wir die Gleichung

$$F(z) = A_0 z^n + A_1 z^{n-1} + \cdots + A_n = 0,$$

wo die Koeffizienten A dem orthoiden Bereiche (A) angehören und A_0 von 0 verschieden ist, also auch unbeschadet der Allgemeinheit gleich Eins gesetzt werden kann. Ist der Bereich

im Sinne des § 3 ein wohldefinierter, so ist die Lösung einer solchen Gleichung im Bereiche (A) als erledigtes Problem zu betrachten; denn einer Lösung $z = \xi_1$ entspricht ein linearer Teiler $z - \xi_1$ der Form $F(z)$ und umgekehrt. Kann man also $F(z)$ in dem (A) entstammenden Formenbereiche in irreduzible Faktoren zerlegen, so entspricht jedem Faktor ersten Grades und nur diesen je eine Lösung.

Liefert aber die Zerlegung von $F(z)$ überhaupt keine Faktoren ersten Grades, so hat die Gleichung $F(z) = 0$ im vorgelegten Bereiche (A) keine Lösung, und dies wird nach den vorhergehenden Erörterungen auch dann schon, wenn der orthoide Bereich (1) ist, für eine unendliche Reihe irreduzibler Formen höheren Grades der Fall sein.

Wir nennen die Gleichung $F(z) = 0$ irreduzibel in (A), wenn die Form $F(z)$ in (A) irreduzibel ist.

Die soeben erörterte Tatsache führt zur Forderung neuer Begriffsbildungen, die im einfachsten Falle schon in den Elementen der Mathematik auftritt, wenn wir in Verbindung mit der „Auflösung" der Gleichung zweiten Grades die reellen quadratischen Irrationalitäten und die komplexen Zahlen einführen.

Diese Forderung kann unmittelbar in folgender Weise formuliert werden.

Es soll der gegebene orthoide Bereich (A) derart erweitert werden, daß die in (A) unlösbare Gleichung $F(z) = 0$ im erweiterten Bereiche lösbar wird; und zwar soll der erweiterte Bereich sämtliche Größen des ursprünglichen Bereichs „enthalten", eine Aussage, deren Inhalt schon am Schlusse des § 13 in Kap. III erörtert wurde.

Dabei genügt es, irreduzible Gleichungen zu betrachten. Denn ist $F_1(z)$ ein irreduzibler Faktor von $F(z)$ und hat die Gleichung $F_1(z) = 0$ im erweiterten Bereiche eine Lösung, so genügt diese auch der Gleichung $F(z) = 0$.

Die neuen Größen, die sich im erweiterten Bereiche, nicht aber in (A) vorfinden, sind die dem Bereiche (A) adjungierten Größen; die Erweiterung des Bereiches selbst be-

steht in der „Adjunktion" dieser neuen Größen; die Gleichung $F(z) = 0$ „wird nach Adjunktion gewisser Größen lösbar." Unsere erste Aufgabe wird es also sein, einer gegebenen irreduziblen Gleichung entsprechende Größen zu finden, deren Adjunktion die Gleichung lösbar macht, und diese Größen in möglichst einfacher Weise zu charakterisieren. Das so gefaßte Gleichungsproblem bietet allerdings auf den ersten Blick nur eine rein formale Aufgabe, ergibt aber in Wirklichkeit eine unermeßliche Erweiterung des Feldes mathematischer Forschung.

§ 6. Wir schreiben die als irreduzibel vorausgesetzte Gleichung $F(z) = 0$, wie schon erwähnt, in der Gestalt

$$z^n + A_1 z^{n-1} + A_2 z^{n-2} + \cdots + A_n = 0$$

und adjungieren — rein formal — die aus je n Größen des Bereichs (A) gebildeten Komplexe

$$\{C'_0, C'_1, \ldots, C'_{n-1}\}, \quad \{C''_0, C''_1, \ldots, C''_{n-1}\}, \ldots$$

(wobei der Leser die Analogie mit der Einführung der komplexen Zahlen, wenn die zu Grunde gelegte Gleichung $z^2 + 1 = 0$ ist, beachten möge). Die Gesamtheit dieser neuen Größen besteht aus allen Komplexen, die man erhält, wenn man den C irgend welche Werte aus (A) beilegt; und zwei derselben, z. B. die ausführlich hingeschriebenen, werden der Definition nach dann und nur dann gleich, wenn die an entsprechenden Stellen stehenden Elemente sämtlich dieselben sind, also $C'_0 = C''_0, \ldots, C'_{n-1} = C''_{n-1}$ ist.

Diese neuen Größen werden zu einem „Bereiche", wenn man ihnen gewisse „Eigenschaften" beilegt, d. h. gewisse Verknüpfungen statuiert, die sogleich als Addition und Multiplikation bezeichnet werden sollen.

Die Definition der Summe und des Produktes zweier Größen

$$\gamma_1 = \{C'_0, C'_1, \ldots, C'_{n-1}\},$$
$$\gamma_2 = \{C''_0, C''_1, \ldots, C''_{n-1}\}$$

sei die folgende:

Man bilde Summe und Produkt der beiden Formen:

$$C_0' + C_1' z + \cdots + C_{n-1}' z^{n-1} \text{ und } C_0'' + C_1'' z + \cdots + C_{n-1}'' z^{n-1}$$

und sodann den Rest, der bei der Division der so entstandenen Formen durch $F(z)$ auftritt:

$$(C_0' + C_0'') + (C_1' + C_1'')z + \cdots + (C_{n-1}' + C_{n-1}'') z^{n-1}$$
$$Q_0 + Q_1 z + \cdots + Q_{n-1} z^{n-1};$$

dann sei

$$\gamma_1 + \gamma_2 = \{(C_0' + C_0''), (C_1' + C_1''), \cdots, (C_{n-1}' + C_{n-1}'')\}$$
$$\gamma_1 \gamma_2 = \{Q_0, Q_1, \ldots, Q_{n-1}\}.$$

Daß die so definierte Addition und Multiplikation kommutativ und associativ, die letztere Operation auch distributiv ist, folgt unmittelbar aus der Tatsache, daß diese Operationen in Wirklichkeit an den entsprechenden Formen ausgeführt werden, wo eben jene Gesetze gelten, und dann die neuen Größen in eindeutiger Weise aus den Koeffizienten der so als Summe oder Produkt erhaltenen Form abgeleitet werden.

Daß die Gleichung $\gamma_1 + \xi = \gamma_2$ immer lösbar ist und immer nur eine Wurzel besitzt, ist auch beinahe unmittelbar klar. Schreibt man ausführlich

$$\xi = \{X_0, X_1, \ldots, X_{n-1}\},$$

so muß

$$C_0' + X_0 = C_0''; \ldots; C_{n-1}' + X_{n-1} = C_{n-1}''$$

sein, d. h. es ist

$$\xi = \{(C_0'' - C_0'), \ldots, (C_{n-1}'' - C_{n-1}')\}.$$

Insbesondere ist die Größe $\{0, 0, \ldots, 0\}$ die „Null" des neuen Bereichs.

Daß ferner die Größe $\{1, 0, 0, \ldots, 0\}$ mit irgend einem γ multipliziert, wieder γ ergibt, folgt aus der Definition der Multiplikation. Diese Größe ist die absolute Einheit des neuen Bereichs und soll sogleich kurz mit 1, sowie die Null mit 0, bezeichnet werden.

Daß auch die Gleichung $\gamma_2 \xi = \gamma$, wenn γ_2 von Null ver-

schieden ist, eine und nur eine Wurzel besitzt, resultiert aus der Irreduzibilität der Form $F(z)$ durch folgende Schlußweise.

Die γ_2 entsprechende Form

$$G(z) = C_0'' + C_1'' z + \cdots + C_{n-1}'' z^{n-1}$$

ist von 0 verschieden, und da $F(z)$ irreduzibel, ist der größte gemeinschaftliche Teiler von $F(z)$ und $G(z)$ der Eins äquivalent. Es ist also die Resultante R von $F(z)$ und $G(z)$ eine von 0 verschiedene Größe des Bereichs (A). Die in Kap. III, § 16 nachgewiesene Relation $R = G_1 F + F_1 G$ kann also durch Division mit R auf die Gestalt

$$(X_0' + X_1' z + \cdots + X_{n-1}' z^{n-1})(C_0'' + C_1'' z + \cdots + C_{n-1}'' z^{n-1}) + (Y_0 + Y_1 z + \cdots + Y_{n-2} z^{n-2}) F(z) = 1 \qquad (D)$$

gebracht werden; und es ist daher der Definition nach, wenn

$$\xi' = \{X_0', X_1', \ldots, X_{n-1}'\}$$

gesetzt wird,

$$\gamma_2 \xi' = 1$$

und für $\xi = \gamma_1 \xi'$ auch

$$\gamma_2 \xi = \gamma_1 .$$

Wäre nun auch $\gamma_2 \eta = \gamma_1$, so folgte hieraus

$$\gamma_2 (\xi - \eta) = 0 ,$$

d. h. das Produkt der γ_2 und $\xi - \eta$ entsprechenden Formen wäre durch $F(z)$ teilbar. Nun ist aber für die γ_2 entsprechende Form $G(z)$, wie schon früher bemerkt, $(F(z), G(z)) \sim 1$; also müßte schon die $\xi - \eta$ entsprechende Form durch $F(z)$ teilbar sein, das ist aber nur ein anderer Ausdruck für die Tatsache $\xi - \eta = 0$, d. h. $\xi = \eta$.

Der Bereich der Größen $\gamma = \{C_0, C_1, \ldots, C_{n-1}\}$ ist demnach wieder ein orthoider Bereich; denn es ist schließlich klar, daß die Größen $1, 1 + 1, \cdots$, die allgemein, ausführlich geschrieben, $\{m, 0, \ldots, 0\}$ sind, niemals die 0 ergeben; dieser Bereich „enthält" den ursprünglich vorgelegten Bereich (A) in der Weise, daß die Größe C aus (A) und die Größe $\{C, 0, \ldots, 0\}$ des neuen Bereichs in allen ihren in Betracht kommenden Eigenschaften übereinstimmen.

Um nun die Größen des neuen Bereichs möglichst einfach zu beschreiben, führen wir für die Größe $\{0, 1, \ldots, 0\}$, wo nur C_1 von 0 verschieden und dieses $= 1$ ist, das einfache Zeichen α ein, und die Ausführung der Multiplikation zeigt dann, daß

$$\alpha^k = \{0, \ldots, 0, 1, 0, \ldots, 0\} \qquad (0 \leqq k \leqq n-1),$$

wo nur das an $k+1^{\text{ter}}$ Stelle stehende Element C_k von 0 verschieden und dieses $= 1$ ist. Es ist ja hierzu nur der Rest der Division von z^k durch $F(z)$ zu bilden.

Dann ist ebenso

$$C_k \alpha^k = \{0, \ldots, 0, C_{k+1}, 0, \ldots, 0\},$$

und also kann $\{C_0, C_1, \ldots, C_{n-1}\}$ nunmehr in der Gestalt

$$C_0 + C_1\alpha + \cdots + C_{n-1}\alpha^{n-1}$$

geschrieben werden.

Um ebenso α^n zu bestimmen, hat man z^n durch $F(z) = z^n + A_1 z^{n-1} + \cdots + A_n$ zu dividieren und erhält

$$z^n = F(z) - A_1 z^{n-1} - \cdots - A_n,$$

also

$$\alpha^n = \{-A_n, -A_{n-1}, \cdots, -A_n\},$$

also

$$\alpha^n + A_1\alpha^{n-1} + \cdots + A_n = 0,$$

und es ist demnach α eine Wurzel der Gleichung im erweiterten Bereiche.

§ 7. Dieser erweiterte orthoide Bereich kann nun kurz dahin charakterisiert werden, daß er durch Adjunktion von α aus (A) entsteht, und soll demgemäß mit (A, α) bezeichnet werden. Er besteht aus allen Größen $C_0 + C_1\alpha + \cdots + C_{n-1}\alpha^{n-1}$, wo die C beliebige Größen des ursprünglichen Bereichs (A) sind; und die Eigenschaften der neuen Größen, d. h. ihre Verknüpfungen nach den vier Species sind in den zu Grunde liegenden Definitionen festgelegt. Aus diesen folgt auch, daß die „Eigenschaften" der dem Bereiche (A) angehörenden Größen, wenn sie als Größen in (A, α) aufgefaßt werden, völlig

unverändert bleiben, d. h. die Addition oder Multiplikation solcher Größen gibt in beiden Fällen dasselbe Resultat. Damit ist auch die unveränderte Übernahme der Zeichen 0 und 1, die schon früher erfolgte, gerechtfertigt.

Die eingeführten Größen mögen als „in Bezug auf (A)“ algebraische Größen bezeichnet werden; sie heißen absolut algebraische Größen oder „algebraische Größen“ — kurzweg, wenn (A) der einem Formenbereiche $[(1), x_1, \ldots, x_m]$ zugeordnete orthoide Bereich ist; man nennt sie endlich algebraische Zahlen, wenn (A) der Bereich der rationalen Zahlen ist.

Die hier durchgeführten Erörterungen haben eine weitgehende prinzipielle Bedeutung. Sie erweisen zunächst die „Existenz“ einer Wurzel α der irreduzibeln Gleichung $F(z) = 0$ in dem genaueren Sinne, daß es einen orthoiden Bereich gibt, der den Bereich (A) und außerdem eine Größe α enthält, für welche $F(\alpha) = 0$ wird. Bei dieser Fassung des Satzes ist die Voraussetzung der Irreduzibilität für $F(z)$ unwesentlich; wir gelangen jedoch, wenn wir diese Voraussetzung festhalten, noch zu den folgenden wichtigen Folgerungen:

Jeder orthoide Bereich, der den Bereich (A) und außerdem eine Größe α enthält, die die Wurzel der in (A) irreduzibeln Gleichung $F(z) = 0$ ist, enthält den ganzen früher definierten Bereich (A, α).

Ein solcher orthoider Bereich enthält jedenfalls alle Größen $C_0 + C_1\alpha + \cdots + C_{n-1}\alpha^{n-1}$, wo die C Größen des Bereichs (A) sind. Summe, Differenz, Produkt und Quotient zweier solcher Größen ergeben sich nun genau nach demselben Bildungsgesetze, wie im Bereiche (A, α); für die ersten drei Fälle ergibt sich dies unmittelbar aus der Definition der Summe und des Produktes in § 6; für den Fall des Quotienten aus der Formel (D) desselben Paragraphen; da die dort mod. $F(z)$ kongruenten Größen, wenn α statt z gesetzt wird, wegen $F(\alpha) = 0$ gleich werden.

Die so gebildeten Größen $C_0' + C_1'\alpha + \cdots + C_{n-1}'\alpha^{n-1}$, $C_0'' + C_1''\alpha + \cdots + C_{n-1}'\alpha^{n-1}$, $\cdots$ sind aber auch alle ver-

schieden, sobald die an entsprechenden Stellen stehenden Koeffizienten nicht durchweg gleich sind. Im entgegengesetzten Falle gäbe es ein System von Größen $K_0, K_1, \ldots, K_{n-1}$ aus (A), für welches

$$K_0 + K_1\alpha + \cdots + K_{n-1}\alpha^{n-1} = 0$$

wäre, ohne daß alle K gleich 0 sind. Nun ist aber der größte gemeinschaftliche Teiler der Formen

$$K(z) = K_0 + K_1 z + \cdots + K_{n-1}z^{n-1}$$

und $F(z)$, da letztere irreduzibel, gleich Eins, und es müßten demnach zwei Formen $F_1(z)$ und $G_1(z)$ existieren, die

$$G_1(z)F(z) + F_1(z)K(z) = 1$$

ergeben. Hieraus würde weiter, wenn man α statt z setzt,

$$F_1(\alpha)K(\alpha) = 1$$

und, da $K(\alpha) = 0$ ist, $1 = 0$ folgen, was in einem orthoiden Bereiche unmöglich ist.

Das erhaltene Resultat läßt sich kurz so aussprechen, daß der früher definierte Bereich (A, α) der „kleinste" orthoide Bereich ist, der, durch Erweiterung von (A) gebildet, eine Wurzel der in (A) irreduzibeln Gleichung $F(z) = 0$ enthält.

Um die erörterte Begriffsbildung an einem einfachsten Beispiel auseinanderzusetzen, ist z. B. die Wurzel α der Gleichung $x^2 = 2$ eine Größe, deren begrifflicher Inhalt vollständig im Bereiche der rationalen und ganzen Zahlen dargelegt wird. Es sind α und $-\alpha$ verschiedene Größen, aber es hätte gar keinen Sinn zu fragen, welche von beiden die positive oder negative Quadratwurzel von 2 bedeutet. Es sind eben α und $-\alpha$ keine Maßgrößen, d. h. keine solchen, die mit einer bestimmten Stelle im Gebiete der reellen — oder auch komplexen Zahlen identifiziert werden. Ist aber umgekehrt $\sqrt{2}$ jene bestimmte positive oder negative reelle Zahl, die in der Analysis als Grenzwert definiert wird, so besitzt diese alle „Eigenschaften" der Größe α, aber darüber hinaus auch solche, die in der Theorie der algebraischen Größen

nicht weiter in Betracht gezogen werden, insbesondere diejenige, daß $\pm\sqrt{2}$ „der Größe nach“ mit jeder rationalen Zahl verglichen werden kann.

Jede in der Theorie der algebraischen Größen entwickelte „Eigenschaft“ von α ist nichts anderes als eine identische Relation, in welche α eingeht, und diese wird auch dann gültig bleiben, wenn man, zu analytischen Betrachtungen übergehend, statt α jenen Grenzwert setzt.

Für den Fall, daß eine algebraische Größe keine algebraische Zahl ist, d. h. wenn in ihre Definition auch Unbestimmte eingehen, werden wir sie auch als algebraische Funktion bezeichnen; der begriffliche Inhalt der „algebraischen Funktion“ ist gegenüber der Analysis genau ebenso enger zu fassen, wie dies für den Fall der Zahl eben auseinandergesetzt wurde.

Hyperorthoide Bereiche.

§ 8. In der Theorie der algebraischen Größen sind prinzipiell algebraische und arithmetische Methoden zu unterscheiden. Dieser prinzipielle Unterschied kann folgendermaßen präcis gefaßt werden.

Die Algebra untersucht die einem orthoiden Bereich entstammenden Formen, in deren Bereiche nicht nur ein größter gemeinschaftlicher Teiler immer existiert, sondern auch — wie wir wissen — durch einen feststehenden Algorithmus in einer endlichen Anzahl von Schritten bestimmt werden kann. Sie benutzt bei dieser Untersuchung keine anderen Faktorenzerlegungen der vorliegenden Formen $F_1, \ldots, F_k$ als jene, die aus der Existenz eines größten gemeinschaftlichen Teilers irgend zweier derselben folgen.

Die Arithmetik untersucht die einem holoiden oder orthoiden Bereiche entstammenden Formen für den Fall, daß diese immer als Produkt einer endlichen Anzahl irreduzibler Formen dargestellt werden können.

In dieser Auffassung — und auch dem Wesen der Sache nach — ist das arithmetische Gebiet das höhere und kann

erst nachdem die algebraischen Methoden ausgebaut sind, erschlossen werden. Für unsre Darstellung der Theorie der algebraischen Größen ist es jedoch kaum ratsam, diese strenge Sonderung der algebraischen und arithmetischen Methoden wirklich durchzuführen, was auch bisher nicht geschehen ist. Dagegen spricht nämlich der gewichtige Umstand, daß man beim Aufbau der hierher gehörigen Begriffe nur von den rationalen, bez. rationalen und ganzen Formen ausgehen kann als solchen, die zuerst allein wirklich gebildet werden, und diese schon zur Definition höherer algebraischer Gebilde herangezogen werden müssen; während doch schon die Untersuchung dieser Formen, ja, selbst die Untersuchung des einfachsten Bereichs der rationalen und ganzen Zahlen die Anwendung „algebraischer" und „arithmetischer" Methoden erheischt.

Trotzdem wird es nicht überflüssig sein, zu zeigen, daß eine solche strenge Sonderung des algebraischen und arithmetischen Teils der Theorie der algebraischen Größen wirklich durchgeführt werden kann. Wenn wir auch in der Folge von der hierzu notwendigen Begriffsbildung keinen Gebrauch machen, soll diese doch kurz durchgeführt werden.

In den vorhergehenden Erörterungen wurde vorausgesetzt, daß der Bereich (A) ein „wohldefinierter" ist, und demgemäß konnte die Gleichung $F(z) = 0$ als irreduzibel angenommen werden. Diese Voraussetzung muß jetzt wegbleiben, und eine Faktorenzerlegung von $F(z)$ darf nur dann zugelassen werden, wenn ein von 1 verschiedener größter gemeinschaftlicher Teiler von $F(z)$ und irgend einer im Laufe einer endlichen Reihe von Operationen sich ergebenden Form $G(z)$ auftritt.

Dann ist aber der in § 6 gebildete Bereich (A, α) im allgemeinen kein orthoider Bereich, da sich die Auflösung der Gleichung $\gamma_2 \xi = \gamma_1$ wesentlich anders stellt.

Entspricht der von 0 verschiedenen Größe γ_2 eine solche Form $G(z) = C_0'' + \cdots + C_{n-1}'' z^{n-1}$, daß $(G(z), F(z)) \sim 1$ wird, so bleiben alle dort geführten Schlüsse gültig, und die Gleichung $\gamma_2 \xi = \gamma_1$ hat eine und nur eine Wurzel.

Ist aber $(G(z), F(z)) \sim D(z)$ eine z wirklich enthaltende Größe, so ist $D(z)$ ein echter Teiler von $F(z)$ (weil $G(z)$ von niedrigerem Grade als $F(z)$ und nicht 0 ist); und daher $F(z) = D(z) \cdot F_1(z)$, $G(z) = D(z) \cdot G_1(z)$. Dann tritt aber an Stelle der Gleichung (D) in § 6 eine Relation:

$$(X_0' + \cdots + X_{n-1}' z^{n-1})(C_0'' + C_1'' z + \cdots + C_{n-1}'' z^{n-1}) + (Y_0 + \cdots + Y_{n-2} z^{n-2}) F(z) = 0;$$

hierin ist

$$X_0' + \cdots + X_{n-1}' z^{n-1} = F_1(z);$$

also können nicht sämtliche Koeffizienten X' verschwinden. Setzt man wieder

$$\xi' = \{X_0', \ldots, X_{n-1}'\},$$

so wird $\gamma_2 \xi' = 0$, trotzdem weder γ_2 noch ξ' Null sind. Es ist γ_2 nach der von Weierstraß eingeführten Ausdrucksweise ein echter Teiler der Null; ob eine Größe γ_2 ein Teiler der Null ist, wird einfach durch Bildung von $D(z) \sim (G(z), F(z))$ entschieden; γ_2 ist ein echter Teiler der Null, wenn $G(z)$ und $F(z)$ einen von 1 verschiedenen größten gemeinschaftlichen Teiler besitzen*).

Ist γ_2 ein echter Teiler der Null, so hat die Gleichung $\gamma_2 \xi = \gamma_1$ entweder gar keine oder unendlich viele Wurzeln. Denn ist ξ_1 irgend eine Wurzel, μ irgend eine Größe des Bereichs (A, α), so wird auch $\gamma_2(\xi_1 + \mu \xi') = \gamma_2 \xi_1 = \gamma_1$.

Weiter wird, wenn γ_2 ein echter Teiler der Null ist, also $\gamma_2 \xi' = 0$, obwohl $\xi' \neq 0$, aus der Existenz einer Größe ξ_1, für die

$$\gamma_2 \xi_1 = \varepsilon,$$

auch

$$\gamma_2 \xi' \xi_1 = \varepsilon \xi' = 0$$

folgen; also muß auch ε ein Teiler der 0 sein; und die Gleichung $\gamma_2 \xi = A$, wo A eine von 0 verschiedene Größe aus (A) be-

*) Ist $F(z)$ irreduzibel, so ist eben 0 der „einzige" Teiler von 0, also gibt es keinen echten Nullteiler; wenn aber $F(z)$ reduzibel ist, gibt es immer echte Teiler der Null.

deutet, besitzt niemals eine Lösung; denn $\gamma_2\xi$ ist nach dem Vorhergehenden ein echter Teiler der Null, A jedoch nicht.

Ebenso hat die Gleichung $\gamma_2\xi = \varepsilon$ keine Lösung, wenn $E(z)$ die ε entsprechende Form und $E(z)$ nicht durch $D(z) \sim (F(z), G(z))$ teilbar ist, denn $\gamma_2\xi_1 - \varepsilon = 0$ bedeutet dieselbe Tatsache, wie die Behauptung, daß

$$(X_0' + \cdots + X_{n-1}' z^{n-1}) G(z) - E(z)$$

durch $F(z)$, also auch durch $D(z)$ teilbar ist.

Ist aber $E(z)$ durch $D(z)$ teilbar, also $E(z) = D(z) E_1(z)$, so bestimmt die Forderung, daß

$$(X_0' + \cdots + X_{n-1}' z^{n-1}) G_1(z) - E_1(z)$$

durch $F_1(z)$ teilbar sei, immer ein System von Koeffizienten X', die nicht sämtlich verschwinden. Denn wegen $(G_1(z), F_1(z)) \sim 1$ hat man jedenfalls zwei von 0 verschiedene Formen Φ und Ψ, für welche

$$\Phi G_1 + \Psi F_1 = 1,$$

also auch

$$\Phi E_1 G_1 + \Psi E_1 F_1 = E_1$$

ist. Hier ist ΦE_1 nicht durch F_1 teilbar, sonst wäre auch E_1 durch F_1 und E durch F teilbar, während doch E nur vom $n-1^{\text{ten}}$ Grade in z ist. Es ist mithin ΦE_1 um so weniger durch F teilbar. Die ΦE_1 entsprechende Größe $\xi_1 = \{X_0', \ldots, X_{n-1}'\}$ besteht daher aus nicht sämtlich verschwindenden Elementen.

In diesem Falle ist demnach eine Größe ξ_1 bestimmt, für welche $\gamma_2\xi_1 = \varepsilon$ wird. Soll dies auch für ξ der Fall sein, also $\gamma_2\xi = \varepsilon$ werden, so muß

$$\gamma_2(\xi - \xi_1) = 0$$

sein, und dies genügt auch. Also muß $\xi - \xi_1$ einer derartigen Form $X(z)$ entsprechen, daß GX durch F teilbar wird. Hierzu ist hinreichend und notwendig, daß $G_1 X$ durch F_1 teilbar sei. Da nun $(F_1, G_1) \sim 1$, muß X durch $F_1(z)$ teilbar sein. Setzt man also $X = F_1(z) \cdot H_1(z)$, wo es genügt, H_1 vom Grade $n-1$ vorauszusetzen, so erhält man alle (und zwar unbegrenzt viele) Größen $\xi - \xi_1$, die der Gleichung $\gamma_1(\xi - \xi_1) = 0$

genügen, und daraus unmittelbar alle der Gleichung $\gamma\xi = \varepsilon$ genügenden Größen.

Man hat daher das folgende allgemeine Resultat:

Es seien die den Größen γ und ε entsprechenden Formen $G(z)$ und $E(z)$; dann hat die Gleichung $\gamma\xi = \varepsilon$ eine und nur eine Lösung, wenn $(G, F) \sim 1$; ist hingegen $(G, F) \sim D$ eine z wirklich enthaltende Form, so hat die Gleichung $\gamma\xi = \varepsilon$ unendlich viele Lösungen oder gar keine, je nachdem $E(z)$ durch D teilbar oder nicht teilbar ist.

§ 9. Um auch hier eine kurze Ausdrucksweise zu erhalten, führen wir für solche Bereiche, die sich vom orthoiden Bereiche nur in Bezug auf die Verhältnisse der Gleichung $\gamma\xi = \varepsilon$ unterscheiden, wieder eine adjektivische Bezeichnung ein.

Ein Bereich heißt hyperorthoid, wenn er ein gewöhnliches Additionsgesetz besitzt, die absolute Einheit enthält, in der Reihe der Größen $1, 1+1, 1+1+1, \ldots$ die Null nicht vorkommt und für den Bereich ein Multiplikationsgesetz besteht, das in Verallgemeinerung des „gewöhnlichen" Multiplikationsgesetzes (Kap. I, § 3) nun kurz folgendermaßen gefaßt werden kann:

a) und *b*) Die Multiplikation ist kommutativ, associativ und distributiv.

c) Die Gleichung $\alpha x = \beta$ hat eine und nur eine Lösung, wenn keine solche von 0 verschiedene Größe δ existiert, für welche $\alpha\delta = 0$. Eine solche Größe α, für welche $\alpha\delta = 0$ ist, ohne daß $\delta = 0$, heißt ein Teiler der Null; ein echter Teiler der Null, wenn sie von 0 verschieden ist.

Der orthoide Bereich ist demnach in der allgemeineren Begriffsbestimmung des hyperorthoiden Bereichs enthalten und entsteht, wenn unter den Größen des Bereichs kein echter Teiler der Null vorhanden ist. Die echten Teiler der Null sind als singuläre Größen anzusehen, und als solche bleibt im orthoiden Bereiche nur die Null zurück.

Die allgemeine Theorie der hyperorthoiden Bereiche soll in diesem Buche nicht weiter erörtert werden; doch ist noch zu bemerken, daß ihre Ausführung*) es ermöglicht, „unendlich kleine“ und „unendlich große“ Größen mit den Methoden und im Rahmen der Theorie der algebraischen Größen zu behandeln.

Wenn der Bereich (A, α) durch eine Gleichung $F(z) = 0$ definiert ist, ohne daß uns Methoden zu Gebote stehen, welche die irreduzibeln Faktoren von $F(z)$ liefern, so kann man trotzdem die dem Bereiche (A, α) entstammenden Formen durch rein algebraische Methoden untersuchen, wie aus den folgenden Betrachtungen hervorgeht.

Insofern unter den Koeffizienten der auftretenden Formen sich kein Teiler der Null befindet, bleiben alle Rechnungsregeln in dem (A, α) entstammenden Formenbereiche genau dieselben wie in dem Falle eines orthoiden Bereichs. Ob nun eine Größe γ Teiler der Null ist, wird durch den größten gemeinschaftlichen Teiler der entsprechenden Formen $G(z)$ und $F(z)$ entschieden. Sobald aber ein solcher auftritt, der im Sinne der Äquivalenz von Eins verschieden ist, ist eben eine Zerlegung von $F(z)$ gegeben, und man wird von $F(z)$ auf dessen Teiler zurückgehen.

Alle in der Folge für eine irreduzible Gleichung $F(z) = 0$ abgeleiteten Resultate bleiben also auch ohne diese Voraussetzung gültig, wenn man nur die Beschränkung festsetzt, daß, sobald unter den Rechnungsgrößen ein Teiler der Null auftritt, man die durch diesen gegebene Faktorenzerlegung von $F(z)$ vornimmt.

Der Galoissche Bereich.

§ 10. Wir setzen wieder den (A) entstammenden Bereich als wohldefiniert voraus; d. h. es ist eine Methode bekannt, mittels welcher jede diesem Bereiche entstammende Form in einer endlichen Anzahl von Schritten in irreduzible Faktoren

*) Siehe auch die Anmerkung zu Kap. V, § 8.

zerlegt werden kann. Die ferneren Untersuchungen gelten also jedenfalls für rationale Formen und weiterhin für alle orthoiden Formenbereiche, in denen wir nachträglich eine solche Zerlegungsmethode festsetzen können.

Es soll jetzt ein solcher erweiterter Bereich konstruiert werden, daß die beliebig gegebene — irreduzible oder reduzible — Form

$$F(z) = z^n + A_1 z^{n-1} + \cdots + A_n$$

in dem erweiterten Bereiche als Produkt linearer Formen darstellbar sei.

Zu diesem Zweck gehen wir von der Form

$$\begin{aligned} P(z) &= (z - x_1)(z - x_2) \cdots (z - x_n) \\ &= z^n - \mathfrak{f}_1 z^{n-1} + \mathfrak{f}_2 z^{n-2} - \cdots + (-1)^n \mathfrak{f}_n \end{aligned}$$

aus. Man bilde mit Hilfe der neuen Unbestimmten $x, u_1, \ldots, u_n$ den Ausdruck

$$\prod_{(i)} (x - u_1 x_{i_1} - u_2 x_{i_2} - \cdots - u_n x_{i_n}) = x^{n!} + \cdots,$$

wo sich das Produktzeichen auf alle Permutationen der Zahlen $1, 2, \ldots, n$ bezieht, von denen eine beliebige durch $i_1, \ldots, i_n$ dargestellt wird. Da dieses Produkt dann eben eine symmetrische Form der Unbestimmten $x_1, \ldots, x_n$ ist, kann es auch in der Gestalt

$$\Pi(x; u_1, \ldots, u_n; \mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_n)$$

geschrieben werden, wo also Π als Symbol einer Form verwendet wird.

Man bilde dann die n Systeme linearer Gleichungen

$$x_{i_r} = \sum_{h=0}^{n!-1} X_h^{(r)} (u_1 x_{i_1} + \cdots + u_n x_{i_n})^h \qquad (\Sigma^{(r)})$$

$$(i_1, \ldots, i_n = 1, 2, \ldots, n;\ i_k \neq i_l),$$

in denen $X_0^{(r)}, \ldots, X_{n!-1}^{(r)}$ als Unbekannte zu betrachten sind, so daß in jedem Systeme $\Sigma^{(r)}$ $(r = 1, \ldots, n)$ die Anzahl der Unbekannten und auch der Gleichungen $n!$ wird.

Nennt man die aus den Koeffizienten der Unbekannten gebildete Determinante $\mathfrak{D}$, so ist $\Theta = \mathfrak{D}^2$ nach Kap. III, § 25 nichts anderes als die Discriminante der Form Π, die nur in den beiden Fällen $n = 2$ oder 3 mit negativem Vorzeichen zu nehmen ist. Es ist also

$$\Theta = \Theta(u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$$

eine bestimmte Form der u und der elementaren symmetrischen Formen $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ und, wie aus der Struktur des Gleichungssystems unmittelbar zu ersehen ist,

$$\Theta X_h^{(r)} = S_h^{(r)}(u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$$

und eben $S_h^{(r)}$ eine in $x_1, \ldots, x_n$ symmetrische Form, also als Form von $u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n$ darstellbar.

Die genauere Gestalt von Θ kann leicht ermittelt werden; es ist Θ, vom Vorzeichen abgesehen, das Produkt aller Faktoren

$$(u_1(x_{i_1} - x_{j_1}) + u_2(x_{i_2} - x_{j_2}) + \cdots + u_n(x_{i_n} - x_{j_n}))^2,$$

wo $i_1, \ldots, i_n$ und $j_1, \ldots, j_n$ alle Wertsysteme durchlaufen, die durch Permutationen der Zahlen $1, 2, \ldots, n$ gegeben sind, aber $i_1, \ldots, i_n$ und $j_1, \ldots, j_n$ verschiedene solche Wertsysteme sind.

Ordnet man Θ nach den Potenzprodukten $U_0, U_1, \ldots, U_t$, so ist jeder Koeffizient (nach Kap. II, § 10) eine symmetrische Form von $x_1, \ldots, x_n$; wird insbesondere Θ als Form der u nach dem lexikographischen Prinzip (Kap. II, § 3) geordnet und ist das Glied mit U_t das höchste, so können wir leicht zeigen, daß der Koeffizient von U_t, vom Vorzeichen abgesehen, eine Potenz von

$$[x_1^{n-1}]^2 = \prod_{r,s}(x_r - x_s)^2 = \Delta \qquad \binom{r, s = 1, \ldots, n}{r < s}$$

ist. Es ist dieser Koeffizient ein Produkt von Faktoren $(x_r - x_s)^2$ und zugleich eine symmetrische Form der x. Der Faktor $x_r - x_s$ tritt demgemäß mit einem geraden Exponenten, z. B $2k$ auf. Ist aber jener Koeffizient als symmetrische Form der Unbestimmten durch $(x_r - x_s)^{2k}$ teilbar, so muß er auch

durch $(x_{r'} - x_{s'})^{2k}$ teilbar sein und umgekehrt; der Exponent $2k$ ist also für jeden Faktor $x_r - x_s$ derselbe, und der Koeffizient ist $[x_1^{n-1}]^{2k}$, wo nur in den Fällen $n = 2$ und 3 das negative Vorzeichen hinzutritt.

Es ist demnach

$$\Theta = \pm \Delta^k U_t + \cdots$$

Setzt man die so bestimmten Werte der Koeffizienten $X_k^{(r)}$ in jene Gleichung des Systems $\Sigma^{(r)}$, in der $i_l = l$ ist, so wird

$$\Theta x_r = \sum_{h=0}^{n!-1} S_h^{(r)} (u_1 x_1 + \cdots + u_n x_n)^h$$

oder

$$\Theta x_r = \varphi^{(r)} (u_1 x_1 + \cdots + u_n x_n;\ u_1, \cdots, u_n;\ \mathfrak{f}_1, \cdots, \mathfrak{f}_n),$$

wo die Symbole $\varphi^{(r)}$ vollständig bestimmte Formen der Größen $u_1 x_1 + \cdots + u_n x_n, u_1, \cdots, u_n, \mathfrak{f}_1, \cdots, \mathfrak{f}_n$ darstellen. Die Gleichung (mit der Unbekannten x)

$$\Theta x_r = \varphi^{(r)} (x, u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$$

hat also die Wurzel $z = u_1 x_1 + \cdots + u_n x_n$, eine Tatsache, die nach Kap. III, § 19 auch durch die Kongruenz

$$\Theta x_r \equiv \varphi^{(r)} (x, u_1, \cdots, u_n, \mathfrak{f}_1, \cdots, \mathfrak{f}_n),\ (\mathrm{mod.}\, x - u_1 x_1 - \cdots - u_n x_n)$$

ausgedrückt wird, wo man nun $r = 1, \ldots, n$ setzen kann. Es wird also auch

$$\Theta^n P(z) = (\Theta z - \Theta x_1) \cdots (\Theta z - \Theta x_n)$$

und

$$\Theta^n P(z) \equiv (\Theta z - \varphi_1) \cdots (\Theta z - \varphi_n),$$
$$(\mathrm{mod.}\, x - u_1 x_{i_1} - \cdots - u_n x_{i_n}),$$

wo φ_k kurz für $\varphi^{(k)}(x, u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ steht.

Es ist mithin

$$\Theta^n P(z) - (\Theta z - \varphi_1) \cdots (\Theta z - \varphi_n)$$

einerseits eine symmetrische Form der Unbestimmten $x_1, \ldots, x_n$, andrerseits durch $x - u_1 x_1 - \cdots - u_n x_n$ teilbar. Sie ist also auch durch $x - u_1 x_{i_1} - \cdots - u_n x_{i_n}$ teilbar, wo $i_1, \ldots, i_n$ eine beliebige Permutation der Zahlen $1, \ldots, n$ bedeutet. Nun

sind $x - u_1 x_{i_1} - \cdots - u_n x_{i_n}$ und $x - u_1 x_{j_1} - \cdots - u_n x_{j_n}$ als lineare Formen auch Primformen und nicht äquivalent, wenn $i_1, \ldots, i_n$ und $j_1, \ldots, j_n$ zwei verschiedene Permutationen bedeuten. Wären sie nämlich äquivalent, so müßte, weil der Koeffizient von x in beiden gleich 1 ist, auch $x_{i_1} = x_{j_1}$ u. s. f. sein.

Jene Form ist also durch das Produkt der Formen $z - u_1 x_{i_1} - \cdots - u_n x_{i_n}$, d. h. durch $\Pi(x; u_1, \ldots, u_n; \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ teilbar, d. h. es ist identisch:

$$\Theta^n P(z) = (\Theta z - \varphi_1) \cdots (\Theta z - \varphi_n) + \mathsf{M}\Pi(x, u_1 \cdots u_n, \mathfrak{f}_1, \cdots, \mathfrak{f}_n).$$

Ordnet man nach den Potenzprodukten der $\mathfrak{f}$, so muß nach dem Gaußschen Prinzip jeder Koeffizient für sich verschwinden, und die Identität bleibt also eine solche, wenn man in ihr

$$\mathfrak{f}_i = (-1)^i A_i$$

setzt. Dann entsteht aber aus $P(z)$ die Form $F(z)$; ferner wird aus Θ eine bestimmte dem Bereiche (A) entstammende Form, die ausführlicher geschrieben

$$T = \pm D^k U_t + \cdots$$

lautet, und in welcher D die Discriminante von $F(z)$ bedeutet. Ebenso gehe $\varphi_1, \ldots, \varphi_n$, M und Π in bestimmte dem Bereiche (A) entstammende Formen der Unbestimmten $x, u_1, \ldots, u_n$ über, die mit $f_1^{(u)}, \ldots, f_n^{(u)} M^{(u)}$, $G^{(u)}$ bezeichnet werden sollen; und man erhält schließlich $T^n F(z)$ gleich

$$\prod_{i=1}^{n} (Tz - f_i^{(u)}(x, u_1, \ldots, u_n)) + M^{(u)} G^{(u)}(x, u_1, \ldots, u_n) \qquad (G^{(u)}),$$

wo

$$G^{(u)} = x^{n!} + \cdots.$$

Sei nun die Discriminante von $F(z)$, d. h. die Größe D von 0 verschieden, so kann man in mannigfacher Weise für die u Wertsysteme bestimmen, z. B. auch solche, die aus rationalen und ganzen Zahlen bestehn, für welche T einen von 0 verschiedenen Wert annimmt; dieser sei t, und beim

Einsetzen dieser Werte der u möge noch $f_i^{(u)}$, $M^{(u)}$, $G^{(u)}$ in f_i, M und $\overline{G}$ übergehn. Dann erhält man schließlich

$$F(z) = \prod_{i=1}^{n}\left(z - \frac{1}{t}f_i(x)\right) + \frac{M}{t^n}\,\overline{G}(x). \qquad (\mathfrak{G})$$

Es sei $G(x)$ irgend ein irreduzibler Faktor von $\overline{G}(x)$; erweitert man dann den Bereich (A) durch Adjunktion einer Wurzel x von $G(x) = 0$ zu (A, α), so wird $\xi_i = \frac{1}{t}f_i(\alpha)$ eine bestimmte Größe des Bereichs, und aus ($\mathfrak{G}$) wird

$$F(z) = \prod_{i=1}^{n}(z - \xi_i),$$

d. h. die Form $F(z)$ ist in der Tat in lineare Faktoren zerlegt; die sämtlichen Wurzeln der Gleichung $F(z) = 0$ sind die Größen $\xi_1, \ldots, \xi_n$, die sämtlich verschieden sind; denn sonst würde $F(z)$ einen mehrfachen echten Teiler enthalten, während doch Dscr. $F(z)$ von 0 verschieden ist.

§ 11. Die Entwicklungen des vorstehenden Paragraphen lassen sich in folgendem Satze zusammenfassen:

Es sei

$$F(z) = z^n + A_1 z^{n-1} + \cdots + A_n$$

und Dscr. $F(z)$ von 0 verschieden. Man bilde die in $x_1, \ldots, x_n$ symmetrische Form

$$\prod_{(i)}(x - u_1 x_{i_1} - \cdots - u_n x_{i_n}),$$

rechne sie in die Gestalt

$$\Pi(x; u_1, \ldots, u_n, \mathfrak{f}_1, \ldots, \mathfrak{f}_n)$$

um und setze $\mathfrak{f}_i = (-1)^i A_i$. Die Discriminante von Π ist dann eine nicht verschwindende Form der u. Man kann demnach für diese (auch rationale und ganze) Wertsysteme bestimmen, so daß Dscr. Π einen von 0 verschiedenen Wert erhält. Setzt man ein solches Wertsystem in Π ein, so erhält man eine Form $\overline{G}(x)$.

Ist $G(x)$ ein irreduzibler Faktor von $\overline{G}(x)$, so entsteht aus (A) durch Adjunktion einer Wurzel x von $G(x) = 0$ ein orthoider Bereich (A, α), in dem die Gleichung n^{ten} Grades $F(z) = 0$ genau n voneinander verschiedene Wurzeln $\xi_1, \ldots, \xi_n$ besitzt, die durch die früher festgesetzte endliche Reihe von Operationen endgültig bestimmt sind, und $F(z)$ ist als Produkt linearer Faktoren

$$F(z) = (z - \xi_1)(z - \xi_2) \cdots (z - \xi_n)$$

dargestellt.

Dabei ist — wie nochmals betont werden soll — $F(z)$ nicht als irreduzibel vorausgesetzt.

Eine weitere wichtige Bemerkung ist die folgende:

Der so erhaltene Bereich (A, α) ist der „kleinste" orthoide Bereich, in welchem $F(z)$ als Produkt linearer Faktoren darstellbar ist, in dem Sinne, daß jeder andere Bereich, der durch Erweiterung von (A) entsteht und in welchem $F(z)$ die erwähnte Eigenschaft besitzt, sämtliche Größen des Bereichs (A, α) enthält.

Sind nämlich in dem angenommenen erweiterten Bereiche $\xi_1, \ldots, \xi_n$ die Wurzeln von $F(z) = 0$, ferner $u_1, \ldots, u_n$ ein den Bedingungen entsprechendes Wertsystem, so ist $u_1\xi_{i_1} + \cdots + u_n\xi_{i_n}$ eine Größe des Bereichs, die sich von α nicht unterscheidet; und der erweiterte Bereich enthält demnach alle Größen des Bereichs (A, α).

Die so definierte Gleichung $G(x) = 0$ ist die Galoissche Resolvente*) der Gleichung $F(z) = 0$ und besitzt die charakteristische Eigenschaft, daß, wenn α eine ihrer Wurzeln bedeutet, für irgend eine Wurzel ξ_i von $F(z) = 0$

$$\xi_i = A_{i0} + A_{i1}\alpha + \cdots + A_{i,m-1}\alpha^{m-1}$$

*) Galois, „Mémoire sur les conditions de la résolubilité des équations par radicaux"; geschrieben 1831, zuerst veröffentlicht in Liouville's Journal, Bd. 11, 1846; dann wieder abgedruckt in den „Oeuvres", Paris 1897. pag. 33. — „Abhandlungen über die algebraische Auflösung der Gleichungen von N. H. Abel und E. Galois". Deutsch herausgeg. von H. Maser. Berlin 1889.

wird, da ξ_i dem Bereiche (A, α) angehört und jede Größe dieses Bereichs in der angegebenen Gestalt geschrieben werden kann.

Da die Gleichung $F(z) = 0$ in dem Bereiche (A, α) n verschiedene Wurzeln besitzt und also $F(z)$ in der Form $P(z)$ geschrieben werden kann, wenn man statt der in § 10 benutzten Zeichen $x_1, \ldots, x_n$ jetzt $\xi_1, \ldots, \xi_n$ setzt, sind die dort gegebenen Entwicklungen nun auch für $F(z)$ gültig, und es sind demnach die Größen $u_1\xi_{i_1} + \cdots + u_n\xi_{i_n}$ durchweg verschieden und sämtlich Wurzeln der Gleichung $\overline{G}(x) = 0$; diese Gleichung vom Grade $n!$ hat ebensoviele verschiedene Wurzeln, die sämtlich dem Bereiche (A, α) angehören. Dasselbe ist also für $G(x) = 0$ der Fall, und auch dann, wenn man statt $G(x)$ irgend einen andern irreduzibeln Faktor von $\overline{G}(x)$ wählt.

Die Galoissche Resolvente besitzt also in jedem Bereiche, in dem sie überhaupt eine Wurzel besitzt, so viele voneinander verschiedene Wurzeln, als ihr Grad Einheiten enthält.

Wesentlich ist noch, daß man in dem zu Beginn dieses Paragraphen gegebenen Satze die $u_1, \ldots, u_n$ als Unbestimmte belassen kann. Denn in der Identität $(G^{(u)})$ des § 10 verschwindet $G^{(u)}(x, u_1, \ldots, u_n)$, wenn man $x = u_1\xi_{i_1} + \cdots + u_n\xi_{i_n}$ setzt, und es wird

$$F(z) = \prod_{i=1}^{n}\left(z - \frac{1}{T} f_i^{(u)}(u_1\xi_{i_1} + \cdots + u_n\xi_{i_n};\, u_1, \cdots, u_n)\right),$$

wo T eine von 0 verschiedene Form ist. Dann müssen aber, da $z - \xi_1, \ldots, z - \xi_n$ sämtliche irreduzible lineare Faktoren von $F(z)$ darstellen, die Größen $\frac{f_i^{(u)}}{T}$, abgesehen von der Reihenfolge, mit $\xi_1, \ldots, \xi_n$ übereinstimmen, also bei Ausrechnung von $\frac{f_i^{(u)}}{T}$ die Unbestimmten $u_1, \ldots, u_n$ von selbst herausfallen.

§ 12. Die Gleichung $\overline{G}(x) = 0$ vom Grade $n!$ hat im Bereiche (A, α) die $n!$ Wurzeln $u_1\xi_{i_1} + \cdots + u_n\xi_{i_n}$, die alle voneinander verschieden sind; die Form $\overline{G}(x)$ ist also in diesem Bereich ein Produkt linearer und nicht äquivalenter Formen; sie besitzt demnach keinen mehrfachen Teiler, und ihre Discriminante ist von 0 verschieden.

Ist für den Bereich (A)

$$\overline{G}(x) = G(x)H(x)\ldots,$$

wo $G, H, \ldots$ irreduzible Formen bedeuten, so müssen auch diese im Sinne der Äquivalenz verschieden sein, da die Discriminante dieselbe Größe, wie früher, demnach wieder von 0 verschieden ist, also auch jetzt kein mehrfacher Teiler existiert.

Die Gleichungen $G(x) = 0, H(x) = 0, \ldots$ können gleichmäßig als Galoissche Resolventen der vorgelegten Gleichung $F(z) = 0$ angenommen werden. Sind $\alpha, \beta, \ldots$ je eine ihrer Wurzeln, so enthält der Bereich (A, α) auch β und ebenso der Bereich (A, β) wieder α. Die Bereiche (A, α), (A, β) sind demnach überhaupt nicht voneinander verschieden; dies folgt übrigens schon aus der Tatsache, daß sowohl (A, α) als auch (A, β) den kleinsten orthoiden Bereich darstellt, der durch Erweiterung von (A) entsteht, und in welchem die Gleichung $F(z) = 0$ n Wurzeln besitzt. Daraus ergibt sich noch leicht der folgende Satz:

Die irreduzibeln Faktoren von $\overline{G}(x)$ im Bereiche (A) sind von gleichem Grade.

Sei $G(x)$ vom Grade k, $H(x)$ vom Grade l. Da β und auch jede Potenz von β dem Bereiche (A, α) angehört, hat man

$$\beta^r = A_{r0} + A_{r1}\alpha + \cdots + A_{r,k-1}\alpha^{k-1}$$
$$(r = 0, 1, \ldots, k)$$

und kann dem Bereiche (A) angehörige Größen $C_0, \ldots, C_k$ bestimmen, die nicht sämtlich verschwinden und den Gleichungen

$$\sum_{r=0}^{k} C_r A_{rs} = 0 \qquad (s = 0, \cdots, k-1)$$

genügen. Es ist

$$C_0 + C_1\beta + \cdots + C_k\beta^k = 0.$$

Da nun die Gleichungen $H(z) = 0$ und

$$C(z) = C_0 + C_1 z + \cdots + C_k z^k = 0$$

die gemeinsame Wurzel β besitzen, haben $H(z)$ und $C(z)$ den gemeinsamen Teiler $z - \beta$, also ist Res. $(H(z), C(z)) = 0$. Wäre der Grad von $H(z)$ größer als k, so würde $H(z)$ im Widerspruche zur Annahme eine in (A) reduzible Form. Es ist also $l \leqq k$; ebenso beweist man, daß $k \leqq l$. Mithin wird in der Tat $k = l$..

Der Grad der Galoisschen Resolvente heißt die Ordnung der Gleichung $F(z) = 0$ im Bereiche (A) und ist demnach für diesen eine bestimmte positive ganze Zahl.

§ 13. Der bisher ausgeschlossene Fall, daß die Discriminante der Gleichung $F(z) = 0$ verschwindet*), läßt sich leicht in die bisherige Betrachtung einfügen.

Die Zerlegung von $F(z)$ in irreduzible Faktoren liefert jedenfalls

$$F = P_1^{a_1} \ldots P_r^{a_r},$$

wo $P_1, \ldots, P_r$ irreduzible Formen bedeuten. Wird die Derivierte nach z durch einen Accent bezeichnet, so ist

$$F' = \sum_{i=1}^{r} a_i \frac{F}{P_i}$$

und hiernach

$$(F(z), F'(z)) \sim D(z) = P_1^{a_1 - 1} \ldots P_r^{a_r - 1},$$

also

$$\frac{F(z)}{D(z)} = P_1 \ldots P_r,$$

eine Form, deren Discriminante nicht verschwindet. Man kann nun für diese Form den Galoisschen Bereich bestimmen, in dem sie, und daher auch $P_1, \ldots, P_r$ in ein Produkt linearer Formen zerfällt; und in diesem Bereiche wird dies auch für F der Fall sein.

*) Als „Discriminante der Gleichung $F(z) = 0$“ bezeichnet man die Discriminante der Form $F(z)$.

Man kann folglich ganz allgemein als Galoisschen Bereich der Gleichung $F(z) = 0$ in Bezug auf den Bereich A den erweiterten Bereich (A, α) verstehn, der durch Adjunktion einer Wurzel α der Galoisschen Resolvente entsteht, die der Gleichung

$$\frac{F(z)}{(F(z), F'(z))} = 0$$

entspricht. Diese Gleichung soll auch allgemein als Galoissche Resolvente der Gleichung $F(z) = 0$ bezeichnet werden.

In diesem Galoisschen Bereiche wird

$$F(z) = (z - \xi_1)^{k_1} \cdots (z - \xi_s)^{k_s},$$

und die Größe ξ_i heißt dann eine k_i-fache Wurzel der Gleichung $F(z) = 0$. Mehrfache Wurzeln existieren dann und nur dann, wenn Dscr. $F(z)$ verschwindet.

Die Gattungsbereiche.

§ 14. Es sei ein bestimmter und wohldefinierter orthoider Bereich (A) vorgelegt, $F(z) = 0$ eine Gleichung, deren Koeffizienten diesem Bereiche angehören, $G(x) = 0$ die Galoissche Resolvente dieser Gleichung. In dem durch Adjunktion einer Wurzel α der Gleichung $G(x) = 0$ erweiterten Bereiche (A, α) zerfällt $F(z)$ in lineare Faktoren, die nach dem Vorhergehenden als gegeben betrachtet werden können. Die Gleichung $F(z) = 0$ hat dann n verschiedene Wurzeln $\xi_1, \ldots, \xi_n$; ist die Discriminante von $F(z)$ von 0 verschieden, so ist n zugleich der Grad der Gleichung $F(z) = 0$; im entgegengesetzten Falle, der im folgenden eingeschlossen, aber ohne Bedeutung ist, wird der Grad größer als n.

Ist

$$f(\xi_1, \ldots, \xi_k)$$

irgend eine Form der Größen ξ mit dem Bereiche (A) angehörigen Koeffizienten, so wird

$$\prod_{(i)} (y - f(\xi_{i_1}, \cdots, \xi_{i_k})),$$

wo das Produkt über alle Permutationen $i_1, \ldots, i_n$ der Zahlen $1, \ldots, n$ auszudehnen ist, eine symmetrische Form der $\xi_1, \ldots, \xi_n$, also eine Form von y mit dem Bereiche (A) angehörigen Koeffizienten. Diese zerfällt in irreduzible Faktoren, von denen jedenfalls einer, gleich 0 gesetzt, eine Gleichung liefert, welche im Bereiche (A, α) die Wurzel $f(\xi_1, \ldots, \xi_k)$ besitzt. Es sei diese Gleichung $\varphi(y) = 0$. Die übrigen Wurzeln von $\varphi(y) = 0$ haben in demselben Bereiche jedenfalls die Gestalt, $f(\xi_{r_1}, \ldots, \xi_{r_k})$, und ihre Anzahl stimmt mit dem Grade von $\varphi(y)$ überein. Bezeichnet man die Wurzeln von $\varphi(y) = 0$ kurz mit $\eta_1, \eta_2, \ldots, \eta_m$, so erhält man, wenn der Bereich (A) durch Adjunktion einer Wurzel η_i von $\varphi(y) = 0$ erweitert wird, nach den Erörterungen in § 7 einen bestimmten orthoiden Bereich (A, η_i), der einfach aus sämtlichen Größen von der Gestalt

$$A_0 + A_1\eta_i + \cdots + A_{m-1}\eta_i^{m-1}$$

besteht. Wir nennen — nach Kroneckers Terminologie*) — den Bereich (A, η_i) einen dem Bereiche (A) entstammenden Gattungsbereich und (A) den Stammbereich von (A, η_i).

Die Bereiche (A, η_1), …, (A, η_m) sind konjugierte Gattungsbereiche; die Größen $\eta_1, \ldots, \eta_m$ — als Wurzeln derselben irreduzibeln Gleichung — und allgemeiner auch die m Größen $A_0 + A_1\eta_i + \cdots + A_{m-1}\eta_i^{m-1}$ $(i = 1, \cdots, m)$ konjugierte Größen; dabei ist selbstverständlich der Ausdruck „konjugiert" in Bezug auf (A) und die Gleichung $\varphi(y) = 0$ zu verstehn, da in einem erweiterten Bereiche die Gleichung $\varphi(y) = 0$ eventuell nicht mehr irreduzibel ist und die dann verschiedenen Faktoren entsprechenden Wurzeln nicht mehr konjugiert sind. — Als spezieller Fall sind hierin die konjugierten Bereiche (A, ξ_i) und die konjugierten Wurzeln der Gleichung $F(z) = 0$ enthalten, wenn $f = \xi_i$ gesetzt wird.

Ein Galoisscher Gattungsbereich ist ein solcher, der „keine konjugierten hat", d. h. für den die kon-

*) Festschrift, § 2.

jugierten $(A, \eta_1), \ldots, (A, \eta_m)$ zusammenfallen. Das ist in der Tat — wie früher (§ 10, 11) bewiesen wurde — immer der Fall, wenn $y = u_1\xi_{i_1} + \cdots + u_n\xi_{i_n}$, oder also die Gleichung $\varphi(y) = 0$ die Galoissche Resolvente ist. Daß umgekehrt die konjugierten zusammenfallen, bedeutet soviel, daß nach Adjunktion einer Wurzel der Gleichung $\varphi(y) = 0$ der erweiterte Bereich auch die übrigen Wurzeln $\eta_2, \ldots, \eta_m$ enthält. Der „kleinste" Bereich, in dem die Gleichung $\varphi(y) = 0$ eine Wurzel besitzt, fällt also mit dem „kleinsten" Bereiche, in dem sie m Wurzeln besitzt, mit dem Galoisschen Bereiche zusammen; der Bereich ist daher ein „Galoisscher Bereich".

Jede Größe des Bereichs (A, η_i) genügt einer in Bezug auf den Bereich (A) irreduzibeln Gleichung, deren Grad ein Teiler des Grades m der Gleichung $\varphi(y) = 0$ ist. Schreibt man jene Größe

$$g(\eta_i) = A_0 + A_1\eta_i + \cdots + A_{m-1}\eta_i^{m-1},$$

so genügt sie jedenfalls der Gleichung

$$H(z) = \prod_{i=1}^{m}(z - g(\eta_i)) = 0,$$

wo das links stehende Produkt symmetrisch in den η_i ist, die Gleichung also jedenfalls die Form

$$z^m + C_0 z^{m-1} + \cdots = 0$$

erhält und dem Stammbereiche (A) angehörige Koeffizienten besitzt.

Ist diese Gleichung irreduzibel, so ist der ausgesprochene Satz richtig. Im entgegengesetzten Falle sei

$$\psi(z) = z^k + C_0' z^{k-1} + \cdots + C_k'$$

ein irreduzibler Faktor der links stehenden Form, dem z. B. die Wurzel $g(\eta_i)$ entspricht. Dann hat die Gleichung

$$\psi(g(y)) = 0$$

die Wurzel η_i mit $\varphi(y) = 0$ gemeinsam. Es ist also

$$\text{Res.}\,(\psi(g(y)), \varphi(y)) = 0$$

und, da $\varphi(y)$ irreduzibel ist, muß

$$\psi(g(y)) = \varphi(y)\varphi_1(y)$$

sein; d. h. der Gleichung $\psi(g(y)) = 0$ entsprechen alle Werte $\eta_1, \ldots, \eta_m$, der Gleichung $\psi(z) = 0$ alle Werte $g(\eta_i)$ als Wurzeln. Da diese Gleichung irreduzibel ist, sind die Wurzeln von $\psi(z) = 0$ alle verschiedenen Werte von $g(\eta_i)$, die selbstverständlich als einfache Wurzeln auftreten. Dies gilt aber für jeden irreduzibeln Faktor von $H(z)$, diese Faktoren sind also von gleichem Grade k, und es ist demnach $m = kl$, wo l die Anzahl der irreduzibeln Faktoren von $H(z)$ bedeutet und $H(z) = (\psi(z))^l$; damit ist aber der ausgesprochene Satz allgemein bewiesen.

§ 15. Eine Größe $g(\eta_i)$ des Bereichs (A, η_i) ist von der k^{ten} Ordnung, wenn sie einer in (A) irreduzibeln Gleichung k^{ten} Grades genügt. Dabei ist immer — nach dem Vorstehenden — k ein Teiler von m, wenn m die Ordnung der Größe η_i bezeichnet.

Konjugierte Größen sind stets von gleicher Ordnung.

Ist die Größe η_i von der m^{ten} Ordnung, so soll auch der Gattungsbereich (A, η_i) von der m^{ten} Ordnung genannt werden; dieser enthält aber auch Größen niedrigerer Ordnung, unter diesen jedenfalls die Größen erster Ordnung, die schon dem Stammbereiche (A) angehören.

Die sämtlichen Größen m^{ter} Ordnung, die in dem Gattungsbereiche m^{ter} Ordnung enthalten sind, bilden in ihrer Gesamtheit eine bestimmte Gattung von in Bezug auf den Stammbereich (A) algebraischen Größen, die wir abermals als von der m^{ten} Ordnung bezeichnen.

Jede Form der Wurzeln $\xi_1, \ldots, \xi_k$ der Gleichung $F(z) = 0$ bestimmt demgemäß einen bestimmten Gattungsbereich und eine bestimmte Gattung von in Bezug auf den Stammbereich (A) algebraischen Größen. Im Gattungsbereiche sind alle Größen der Gattung enthalten. Der Gattungsbereich enthält

aber auch andere, „niedrigere" Gattungen, und zwar in der Weise, daß, wenn er irgend eine Größe k^{ter} Ordnung γ enthält, er auch sämtliche Größen der durch diese definierten Gattung enthält. Denn diese sind ja von der Gestalt $A_0 + A_1\gamma + \cdots + A_{k-1}\gamma^{k-1}$, wo γ der Annahme nach in ähnlicher Weise durch η_i ausdrückbar ist.

Diese Bestimmungen dehnen sich unmittelbar auf die „rationalen Funktionen der Wurzeln von $F(z) = 0$" aus, d. h. auf Größen

$$\frac{f_1(\xi_1, \ldots, \xi_k)}{f_2(\xi_1, \ldots, \xi_k)}$$

aus, wo $f_2(\xi_1, \ldots, \xi_k)$ von 0 verschieden. Multipliziert man nämlich mit den konjugierten Größen von $f_2(\xi_1, \ldots, \xi_k)$ in Zähler und Nenner, so wird, wenn die Gleichung für $f_2(\xi_1, \ldots, \xi_k)$:

$$z^k + C_1 z^{k-1} + \cdots + C_k = 0$$

lautet, der Nenner C_k sein, und dieser Koeffizient ist nicht 0, weil diese Gleichung sonst reduzibel wäre, und jener Ausdruck ist damit unmittelbar auf die Gestalt $f(\xi_1, \ldots, \xi_k)$ zurückgeführt.

Jede Größe m^{ter} Ordnung γ, die in dem Gattungsbereiche m^{ter} Ordnung (A, η_i) enthalten ist, bestimmt diesen Gattungsbereich und die in ihm enthaltene Gattung m^{ter} Ordnung in gleicher Weise.

Dieser Satz kann so formuliert werden, daß, wenn γ und η_i von der m^{ten} Ordnung sind und γ in (A, η_i) enthalten ist, die Gattungsbereiche (A, γ) und (A, η_i) dieselben Größen enthalten.

Der Annahme nach ist auch jede Potenz von γ in (A, η_i) enthalten, also

$$\gamma^r = A_{r0} + A_{r1}\eta_i + \cdots + A_{r\,m-1}\eta_i^{m-1};$$
$$(r = 0, 1, \ldots, m-1)$$

und die Determinante $|A_{rs}|$ kann nicht verschwinden; denn aus $|A_{rs}| = 0$ würde die Existenz eines dem Bereiche (A) angehörigen Größensystems $C_r (r = 0, \cdots, m-1)$ folgen, dessen Elemente nicht sämtlich Null sind, und den Gleichungen

$$\sum_{r=0}^{m-1} C_r A_{rs} = 0 \qquad (s = 0, \ldots, m-1)$$

genügen. Dann wäre aber auch

$$C_0 + C_1\gamma + \cdots + C_{m-1}\gamma^{m-1} = 0$$

und γ keine Größe m^{ter} Ordnung. Ist aber nun $|A_{rs}|$ nicht 0, so erhält man aus den Gleichungen für γ^r auch

$$\eta_i = B_0 + B_1\gamma + \cdots + B_{m-1}\gamma^{m-1},$$

d. h. es ist η_i und damit jede Größe des Gattungsbereichs (A, η_i) auch in (A, γ) enthalten.

Endlich erkennt man noch unmittelbar, daß, wenn die Größe α im Gattungsbereiche (A, η_i) enthalten ist, auch alle Größen der Gattung von α und des Gattungsbereichs (A, α) in (A, η_i) enthalten sind.

Die Gattung von α ist, wenn α eine Größe k^{ter} Ordnung, die einzige im Gattungsbereiche (A, α) enthaltene Gattung k^{ter} Ordnung.

Die Gattung von α ist unter der Gattung von β enthalten, wenn ihre sämtlichen Größen Größen des Gattungsbereichs (A, β) sind.

Gattungsbereiche, deren Stammbereich selbst schon ein Gattungsbereich ist.

§ 16. Es sei wieder (A) der orthoide Bereich, von dem wir ausgehn; $F(z)$ irgend eine dem Bereiche (A) entstammende irreduzible Form, und $\xi_1, \ldots, \xi_n$ die Wurzeln der Gleichung $F(z) = 0$ in dem entsprechend erweiterten Bereiche. Dann ist der Gattungsbereich (A, ξ_i) abermals ein orthoider Bereich, der als neuer Ausgangspunkt für die bisher entwickelte Begriffsbildung dienen kann, so daß (A, ξ_i) jetzt die bisher von (A) eingenommene Rolle erhält. Dies führt zur Bildung von Gattungsbereichen, deren Stammbereich selbst schon ein Gattungsbereich ist, die also, wenn sie von den bisher betrachteten Gattungsbereichen „ersten Ranges“ verschieden

wären, Gattungsbereiche „höheren Ranges“ darstellen würden. Es wird sich aber das wichtige Resultat ergeben, daß die aus dem Stammbereiche (A) gebildeten Gattungsbereiche schon eine in sich abgeschlossene Gesamtheit bilden; d. h., wenn man von einem Gattungsbereich als Stammbereich ausgeht, der so entstehende Gattungsbereich „höheren Ranges“ nichts anderes als ein aus (A) entstammender Gattungsbereich ist.

Bevor wir aber hierauf näher eingehen, muß gezeigt werden, daß die Begriffsbildung, die zu einem aus (A, ξ_i) entstammenden Gattungsbereiche aufsteigt, in der Tat sich vollständig unter die Entwicklungen der §§ 14, 15 einreiht. Dies ist der Fall, wenn wir folgenden Satz beweisen können.

Mit (A) ist immer auch der Gattungsbereich (A, ξ_i) ein wohldefinierter orthoider Bereich.

Nach den Festsetzungen in § 3 dieses Kapitels ist darunter, ausführlicher formuliert, Folgendes zu verstehen. Mit jener Methode, die es ermöglicht, in einer endlichen Anzahl von Schritten die irreduzibeln Faktoren irgend einer aus (A) entstammenden Form zu bestimmen, ist immer zugleich eine Methode gegeben, die dasselbe Problem für irgend eine aus dem Gattungsbereiche (A, ξ_i) entstammende Form vollständig erledigt. Diese Methode soll nun ausführlich dargelegt werden.*)

Hierzu dienen zuerst die folgenden vorläufigen Bemerkungen.

Es sei die Form — die in Bezug auf eine der Unbestimmten x als regulär angenommen werden kann und soll —

$$\Phi^{(i)}(x) = x^n + \alpha_1^{(i)} x^{n-1} + \cdots + \alpha_n^{(i)}$$

gegeben, wo $\alpha_r^{(i)}$ dem Gattungsbereiche (A, ξ_i) entstammende Formen der übrigen Unbestimmten sind, also ausführlich

$$\alpha_r^{(i)} = A_{r0} + A_{r1}\xi_i + \cdots + A_{r\,m-1}\xi_i^{m-1}$$

und demnach A_{rs} wieder dem orthoiden Bereiche (A) entstammende Formen bedeuten. Diese Form $\Phi^{(i)}$ sei in Fak-

*) Zuerst von Kronecker angegeben in § 4 der „Festschrift“. Siehe auch die früher citierte Abhandlung von Molk (Acta math. Bd. VI).

toren zu zerlegen, die im Gattungsbereiche (A, ξ_i) irreduzibel sind. Die Bezeichnungen $\Phi^{(i)}$ und $\alpha_r^{(i)}$ sind deshalb notwendig, weil wir die „konjugierten Formen“*) $\Phi^{(1)}, \ldots, \Phi^{(m)}$ zugleich betrachten müssen.

Die Existenz einer solchen Zerlegung

$$\Phi^{(i)}(x) = P_1^{(i)}(x) \ldots P_k^{(i)}(x) \qquad (a)$$

und auch die volle Eindeutigkeit dieser Zerlegung, wenn der Koeffizient der höchsten Potenz von x in jedem irreduzibeln Faktor $P_i^{(i)}$ gleich Eins ist, sind in § 3 dieses Kapitels nachgewiesen; es kommt nur darauf an, diese Faktoren wirklich zu bestimmen. Ferner ist auch klar, daß jene Faktorenzerlegung sich zu gleicher Zeit für die konjugierten Formen in den konjugierten Gattungsbereichen ergibt; da ja für ξ_i nur die Voraussetzung eintritt, daß diese Größe eine Wurzel der in (A) irreduzibeln Gleichung $F(z) = 0$ ist, also die Resultate für $i = 1, \ldots, m$ gleichmäßig gelten.

Setzt man $x = u\xi_i + v$, wo u und v neue Unbestimmte sind, so ist auch

$$\Phi^{(i)}(u\xi_i + v) = P_1^{(i)}(u\xi_i + v) \ldots P_k^{(i)}(u\xi_i + v), \qquad (b_1)$$

und umgekehrt folgt aus einer Zerlegung von $\Phi^{(i)}(u\xi_i + v)$:

$$\Phi^{(i)}(u\xi_i + v) = Q_1^{(i)}(u, v) \ldots Q_i^{(i)}(u, v) \qquad (b_2)$$

wenn man wieder $u\xi_i + v = x$ setzt,

$$\Phi^{(i)}(x) = Q_1^{(i)}(u, x - \xi_i u) \ldots Q_i^{(i)}(u, x - \xi_i u)$$

eine Zerlegung von $\Phi^{(i)}(x)$; denn diese Form kann durch keine Form teilbar sein, welche die Unbestimmte u wirklich enthält; es muß also aus $Q_i^{(i)}(u, x - \xi_i u)$ die Unbestimmte u von selbst herausfallen.

In der Faktorendarstellung (a) und (b_1) oder (b_2) von $\Phi^{(i)}(x)$ und $\Phi^{(i)}(u\xi_i + v)$ müssen endlich die Faktoren $P_i^{(i)}(x)$ und $P_i^{(i)}(u\xi_i + v)$ zugleich irreduzibel sein; denn aus einer

*) Konjugierte Formen sind solche Formen, die in gleicher Weise aus konjugierten Koeffizientenreihen aufgebaut werden.

wirklichen Zerlegung der einen Form folgt nach dem eben Gesagten eine ebensolche für die andere Form.

§ 17. Wir führen nun die Betrachtung in dem durch die Gleichung $F(z) = 0$ definierten Galoisschen Bereiche weiter, der die Größen $\xi_1, \ldots, \xi_m$ sämtlich enthält. Dann ist aber für irgend zwei der Formen

$$\Phi^{(i)}(u\xi_i + v) \qquad (i = 1, \ldots, m)$$

der größte gemeinschaftliche Teiler ~ 1. (Um eben diese Vereinfachung des Problems zu erreichen, muß im allgemeinen die Transformation $x = u\xi_i + v$ benutzt werden). Ist nämlich, ausführlich geschrieben,

$$\Phi^{(i)}(u\xi_j + v) = (u\xi_i + v)^n + \alpha_1^{(i)}(u\xi_i + v)^{n-1} + \cdots + \alpha_n^{(i)},$$
$$\Phi^{(j)}(u\xi_j + v) = (u\xi_j + v)^n + \alpha_1^{(j)}(u\xi_j + v)^{n-1} + \cdots + \alpha_n^{(j)},$$

so wird weiter, wenn man $u\xi_i + v = w$ setzt,

$$u\xi_j + v = w + u(\xi_j - \xi_i)$$

und demnach

$$\Phi^{(i)}(w) = w^n + \alpha_1^{(i)} w^{n-1} + \cdots + \alpha_n^{(i)}$$
$$\Phi^{(j)}(w + u(\xi_j - \xi_i)) = (w + u(\xi_j - \xi_i))^n + \alpha_1^{(j)}(w + u(\xi_j - \xi_i))^{n-1} + \cdots \alpha_n^{(j)},$$

und der größte gemeinschaftliche Teiler dieser transformierten Form ist dann und nur dann Eins, wenn dies für die ursprünglichen Formen der Fall war. Daß aber für diese transformierten Formen in der Tat

$$(\Phi^{(i)}(w),\ \Phi^{(j)}(w + u(\xi_j - \xi_i))) \sim 1$$

ist, wird aus der Bemerkung evident, daß dieser größte gemeinschaftliche Teiler, als Teiler von $\Phi^{(i)}(w)$, nur eine Form sein kann, welche die Unbestimmte u nicht enthält, und also, wenn man $\Phi^{(j)}(w + u(\xi_j - \xi_i))$ nach Potenzen von u ordnet, den Koeffizienten jeder Potenz von u, also auch den Koeffizienten von u^n, d. i. die Größe

$$(\xi_j - \xi_i)^n$$

teilen muß. Da aber diese Größe von 0 verschieden ist und von den Unbestimmten frei ist, muß der angenommene größte gemeinschaftliche Teiler ~ 1 sein.

Wir können nun weiter voraussetzen, daß Dscr. $\Phi^{(i)}(x)$ von 0 verschieden, also $\Phi^{(i)}(x)$ keinen mehrfachen Teiler besitzt, da sonst eine Zerlegung $\Phi^{(i)} = \Phi_1^{(i)} \Phi_2^{(i)}$ bekannt und die weitere Arbeit an diesen Faktoren ausgeführt werden kann.

Dann ist endlich

$$\prod_{i=1}^{m} \Phi^{(i)}(u\xi_i + v) = G(u, v)$$

eine dem Bereiche (A) entstammende Form der Unbestimmten u, v und der übrigen x, die keinen mehrfachen Teiler besitzt; denn irgend ein irreduzibler mehrfacher Teiler müßte ein mehrfacher Teiler einer Form $\Phi^{(i)}$, oder ein gemeinschaftlicher Teiler von $\Phi^{(i)}$ und $\Phi^{(j)}$ sein, während doch keiner der beiden Fälle stattfindet.

Zerlegt man nun die Form $G(u, v)$, die dem wohldefinierten Bereiche (A) entstammt, in diesem Bereiche in irreduzible Faktoren

$$G(u, v) = G_1(u, v)\, G_2(u, v) \ldots G_s(u, v),$$

so wird im Bereiche (A, ξ_i)

$$(\Phi^{(i)}(u\xi_i + v),\ G_r(u, v)) \sim Q_r^{(i)}(u, v)$$

ein irreduzibler echter Teiler von $\Phi^{(i)}$ sein. Es kann zuerst $Q_r^{(i)} \sim 1$ nicht stattfinden, sonst wäre auch

$$(\Phi^{(i)}(u\xi_i + v),\ G_r(u, v)) \sim 1 \qquad (i = 1, \ldots, m)$$

und demnach

$$(G,\ G_1) \sim 1$$

während doch G_1 ein von 1 verschiedener Teiler der Form G ist.

Es kann aber auch nicht

$$Q_r^{(i)} = Q_{r1}^{(i)} Q_{r2}^{(i)}$$

d. i. das Produkt zweier echter Teiler sein; denn $Q_r^{(i)}$ ist für

$i \neq 1, \ldots, m$ immer ein Teiler von $\Phi^{(i)}(u\xi_i + v)$ und, da $(\Phi^{(i)}, \Phi^{(j)}) \sim 1$, ist demnach auch $(Q_r^{(i)}, Q_r^{(j)}) \sim 1$. Da nun G_r durch $Q_r^{(i)}$ für $i = 1, \ldots, m$ teilbar ist, muß G_r auch durch $\prod_{i=1}^{m} Q_r^{(i)}$ teilbar sein. Es wäre demnach

$$G_r = \prod_{i=1}^{m} Q_{r1}^{(i)} \prod_{i=1}^{m} Q_{r2}^{(i)} \ldots$$

das Produkt zweier wirklichen Formen aus (A); denn mit $Q_{r1}^{(i)}$ enthält auch das Produkt dieser Formen die Unbestimmten.

Wendet man dieses Verfahren auf sämtliche Formen $G_1(u, v), \ldots, G_s(u, v)$ an, so erhält man alle irreduzibeln Teiler von $\Phi^{(i)}(u, v)$; denn jeder solcher muß in einer der Formen $G_1, \ldots, G_s$ als Teiler enthalten sein.

Die irreduzibeln Teiler $Q_r^{(i)}(u, v)$ $(r = 1, \ldots, s)$ sind auch sämtlich verschieden; sonst hätten — im Widerspruche mit unsern Entwicklungen — G_r und $G_{r'}$ einen gemeinschaftlichen, also G einen mehrfachen Teiler.

Weiter ist jeder irreduzible Teiler von $\Phi^{(i)}$ in einer und nur einer der Formen G_r enthalten, also

$$\Phi^{(i)}(u\xi_i + v) = Q_1^{(i)}(u, v), \ldots, Q_s^{(i)}(u, v)$$

und endlich, wieder $u\xi_i + v = x$ gesetzt:

$$\Phi^{(i)}(x) = P_1^{(i)}(x) \ldots P_s^{(i)}(x),$$

da in den Formen rechts, wenn man $v = x - u\xi_i$ setzt, u von selbst herausfallen muß.

Die Zerlegung einer Form $\Phi^{(i)}(x)$, deren Discriminante von 0 verschieden ist, in irreduzible Faktoren für den Gattungsbereich (A, ξ_i) geschieht daher nach folgender Regel.

Man bilde die Form $\prod_{i=1}^{m} \Phi^{(i)}(u\xi_i + v) = G(u, v)$, deren Koeffizienten dem Bereiche (A) angehören, und zerlege G nach den für (A) geltenden Methoden:

$$G = G_1 G_2 \ldots G_s.$$

Ist alsdann

$$(\Phi^{(i)}(u\xi_i + v),\ G_r(u, v)) \sim Q_r^{(i)}(u, v),$$

so wird

$$\Phi^{(i)}(u\xi_i + v) \sim Q_1^{(i)}(u, v) \dots Q_s^{(i)}(u, v)$$

oder, wenn wieder $u\xi_i + v = x$ gesetzt wird:

$$\Phi^{(i)}(x) \sim Q_1^{(i)}(u, x - u\xi_i) \dots Q_s^{(i)}(u, x - u\xi_i) \sim P_1^{(i)}(x) \dots P_s^{(i)}(x)$$

die gesuchte Zerlegung.

§ 18. Die soeben entwickelte Methode, die die Zerlegung der dem Gattungsbereiche (A, ξ_i) entstammenden Form $\Phi^{(i)}$ in irreduzible Faktoren liefert, ist, wie ihre Darstellung zeigt, von der Anzahl der in der Form auftretenden Unbestimmten prinzipiell völlig unabhängig. Es mag jedoch erwähnt werden, daß man für den Fall, wo die Form mehr als eine Unbestimmte enthält, nach den Erörterungen in Kap. II, § 4 von $\Phi^{(i)}$ zu der dort definierten entsprechenden Form einer Unbestimmten $\varphi^{(i)}$ übergehen kann; die in endlicher Anzahl vorhandenen Teiler von $\varphi^{(i)}$ ergeben dann sämtliche Teiler von $\Phi^{(i)}$, also auch die Zerlegung dieser Form in irreduzible Teiler.

Zwischen Formen einer Unbestimmten und solchen, die mehrere Unbestimmte enthalten, existiert jedoch ein prinzipieller Unterschied anderer Art, der hier noch erörtert werden muß.

Eine aus (A) entstammende irreduzible Form kann reduzibel werden oder auch irreduzibel bleiben, je nachdem wir verschiedene aus (A) entstammende Gattungsbereiche (A, ξ_i) zu Grunde legen. Enthält aber die betrachtete Form nur eine Unbestimmte, so ist der entsprechende Galoissche Bereich ein solcher, in welchem jene Form unbedingt in lineare Faktoren zerlegbar ist.

Wir nennen nun eine Form, die aus (A) entstammt, absolut irreduzibel, wenn sie in jedem aus (A) entstammenden Gattungsbereiche irreduzibel bleibt.

Nicht lineare Formen einer Unbestimmten sind demnach niemals absolut irreduzibel. Wirkliche lineare Formen sind selbstverständlich immer absolut irreduzibel.

Ist eine Form mehrerer Unbestimmten $\Phi^{(i)}$ reduzibel, so muß dasselbe auch für die entsprechende Form einer Unbestimmten $\varphi^{(i)}$ der Fall sein, und die Zerlegung in irreduzible Faktoren muß schon in dem der Gleichung $\varphi^{(i)} = 0$ entsprechenden Galoisschen Bereiche durchgeführt werden können; denn die irreduzibeln Faktoren müssen solchen Faktoren von $\varphi^{(i)}$ entsprechen, in denen die Exponenten der Unbestimmten als „Höhenzahlen" möglich sind.

Wenn also $\Phi^{(i)}$ reduzibel ist, so kann die Zerlegung immer schon in einem von vornherein bestimmten Gattungsbereich ausgeführt werden.

Nun kann es aber vorkommen, daß keiner der Faktoren von $\varphi^{(i)}$ der angegebenen Bedingung genügt, also $\Phi^{(i)}$ in jenem Galoisschen Bereich irreduzibel bleibt; und dann muß $\Phi^{(i)}$ auch absolut irreduzibel sein. Dieser Fall wird in der Tat bei Formen beliebigen Grades vorkommen, wenn die Anzahl der Unbestimmten größer als Eins ist. Ist $F(x_1, \ldots, x_{m-1})$ eine beliebige Form, so wird

$$F(x_1, \ldots, x_{m-1}) + x_m$$

eine Form von der eben angegebenen Beschaffenheit sein. Denn, da sie in x_m linear ist, muß, wenn sie überhaupt zerlegbar ist, ein echter Teiler existieren, der x_m nicht enthält. Dieser muß aber dann auch ein Teiler des Koeffizienten von x_m, d. i. ein Teiler der Einheit sein, und wäre also — im Widerspruche zur Annahme — doch kein echter Teiler. Wir haben also folgenden Satz gewonnen:

Im Bereiche der aus (A) entstammenden Formen gibt es absolut irreduzible Formen beliebiger Dimension, die aber zumindest zwei Unbestimmte enthalten.

Ob eine Form $\Phi^{(i)}$ absolut irreduzibel ist, wird durch ihre Untersuchung in dem der Gleichung $\varphi^{(i)} = 0$ entsprechenden Galoisschen Bereiche entschieden. $\Phi^{(i)}$ ist dann und nur dann absolut irreduzibel, wenn sie in dem durch $\varphi^{(i)} = 0$ definierten Galoisschen Bereiche irreduzibel ist.

§ 19. Ist (A, ξ_i) ein durch irgend welche Wurzel der in (A) irreduzibeln Gleichung $F(z) = 0$ definierter Gattungsbereich und $G_i(z) = 0$ wieder eine in (A, ξ_i) irreduzible Gleichung n^{ten} Grades, η_{ij} eine ihrer Wurzeln, so wird $(\mathsf{A}, \xi_i, \eta_{ij})$ ein Gattungsbereich, dessen Stammbereich (A, ξ_i) ist. Er besteht aus sämtlichen Größen

$$\sum_{r=0}^{n-1} \alpha_r^{(i)} \eta_{ij}^r ;$$

oder, wenn man die ausführliche Form von $\alpha_r^{(i)}$ einführt, aus sämtlichen Größen:

$$g(\xi_i, \eta_{ij}) = \sum_{s=0}^{m-1} \sum_{r=0}^{n-1} A_{rs} \xi_i^s \eta_{ij}^r .$$

Bildet man nach Einführung zweier neuer Unbestimmten u und v die Formen*)

$$u\xi_i + v\eta_{ij} \qquad (i = 1, \ldots, m;\ j = 1, \ldots, n),$$

so sieht man, daß zwei solche Formen $u\xi_i + v\eta_{ij}$ und $u\xi_{i'} + v\eta_{i'j'}$ dann und nur dann gleich werden können, wenn $i = i'$ und $j = j'$ ist. Man kann daher (nach Kap. II. § 17) zwei dem Bereiche (A) angehörige Größen, unter anderen auch rationale und ganze Zahlen k und l so bestimmen, daß

$$\gamma_{ij} = k\xi_i + l\eta_{ij} \quad (i = 1, \ldots, m;\ j = 1, \ldots, n)$$

mn verschiedene Größen sind. Diese genügen demnach der Gleichung

$$\prod_{i=1}^{m} \prod_{j=1}^{n} (z - \gamma_{ij}) = H(z) = 0,$$

wo $H(z)$ eine dem Bereiche (A) entstammende Form ist; denn $\prod_{j=1}^{n} (z - \gamma_{ij})$ ist symmetrisch in Bezug auf $\eta_{i1}, \ldots, \eta_{in}$, also eine Form des Bereichs (A, ξ_i), und $H(z)$ demnach weiter symmetrisch in Bezug auf $\xi_1, \ldots, \xi_m$.

*) Die weitere Entwicklung geschieht demnach im Galoisschen Bereiche der Gleichung $F(z)\, G_1(z) \ldots G_m(z) = 0$.

Irgend eine Größe $g(\xi_i, \eta_{ij})$ des Bereichs (A, ξ_i, γ_{ij}) kann stets auf die Gestalt

$$g(\xi_i, \eta_{ij}) = C_0 + C_1\gamma_{ij} + \cdots + C_{mn-1}\gamma_{ij}^{mn-1} \qquad (g)$$

gebracht werden, wo die Größen C dem Bereiche (A) angehören. Es repräsentiert nämlich (g), wenn $i = 1, \ldots, m$; $j = 1, \ldots, n$ gesetzt wird, ein Gleichungssystem, aus welchem die „Unbekannten" C sich als Größen des Bereichs (A) ergeben. Jedenfalls ist

$$\Delta C_s = \Delta_s,$$

wo sämtliche Determinanten $\Delta, \Delta_1, \ldots \Delta_{mn-1}$ von folgender Gestalt

$$|g_h(\xi_i, \eta_{ij})| \qquad \begin{pmatrix} h = 1, \ldots, mn \\ i = 1, \ldots, m;\ j = 1, \ldots, n \end{pmatrix}$$

sind und

$$g_h(\xi_i, \eta_{ij}) = \sum_{s=0}^{m-1} \sum_{r=0}^{n-1} A_{rs}^{(h)} \xi_i^s \eta_{ij}^r$$

geschrieben werden kann. Dabei ist Δ von 0 verschieden, weil Δ^2 die Discriminante von $H(z)$ und $H(z) = 0$ eine Gleichung mn^{ten} Grades mit mn verschiedenen Wurzeln ist.

Bei jener Darstellung von $g_h(\xi_i, \eta_{iy})$ wird aber nach dem Multiplikationssatz für Determinanten

$$|g_h(\xi_i, \eta_{ij})| = |A_{rs}^{(h)}| \, |\xi_i^s \eta_{ij}^r|$$

und $|\xi_i^s \eta_{ij}^r|$ nicht 0, weil sonst auch Δ gleich 0 wäre.*) Es ist also, nach Weglassung von $|\xi_i^s \eta_{ij}^r|$, in der Tat

$$KC_s = K_s$$

wo $K, K_1, \ldots, K_{mn-1}$ aus Größen des Bereichs (A) gebildete Determinanten sind und K von 0 verschieden ist.

Damit ist aber nachgewiesen, daß der Gattungsbereich (A, ξ_i, η_{ij}) mit dem Gattungsbereich (A, γ_{ij}) identisch ist, der durch Adjunktion einer Wurzel von $H(z) = 0$ aus

*) Die Auswertung der Determinante $|\xi_i^s \eta_{ij}^r|$ ergibt sich unmittelbar nach der in Kap. II. § 12 benutzten Methode.

dem Stammbereiche (A) entsteht. Denn jede Größe $g(\xi_i, \eta_{ij})$ ist nach (g) in (A, γ_{ij}) enthalten, und umgekehrt jede Größe dieses Bereichs in (A, ξ_i, η_{ij}), weil das für γ_{ij} der Fall ist.

Die Gesamtheit der aus dem Stammbereiche (A) entstehenden Gattungsbereiche bildet daher ein in sich geschlossenes Größenreich, insofern es durch Adjunktion der Wurzeln einer solchen Gleichung, deren Koeffizienten einem solchen Gattungsbereiche angehören, nicht mehr erweitert werden kann.

Das einfachste Größenreich dieser Art ist das Reich der algebraischen Zahlen, insofern nach dem eben Bewiesenen jede Gleichung, deren Koeffizienten algebraische Zahlen sind, wieder nur algebraische Zahlen im gewöhnlichen Sinne des Wortes (§ 7 dieses Kap.) definiert. Ebenso entsteht das Reich der algebraischen Funktionen von n Unbestimmten.

Es gibt demnach nur algebraische Größen (Zahlen und Funktionen) „ersten Ranges", wenn wir diese nun überflüssig gewordene Bezeichnung noch einmal in dem Sinne der einleitenden Worte zu § 16 anwenden.

Jene Gleichung $H(z) = 0$, welche die betreffende algebraische Größe direkt als (A) entstammend definiert, kann nach der gegebenen Anweisung unmittelbar gebildet werden.

Die Rationalitätsbereiche.

§ 20. Es seien

$$\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_\mu$$

irgend welche einem bestimmten holoiden oder orthoiden Bereich angehörige Größen. Dann bildet die Gesamtheit der rationalen und ganzen Formen von $\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu$, wie man unmittelbar sieht, einen (echten oder unechten) holoiden Bereich.

Die Gesamtheit der „rationalen Funktionen von $\mathfrak{R}_1, \ldots \mathfrak{R}_\mu$", d. h. der Quotienten zweier rationalen und ganzen Formen dieser

Größen, wobei nur die Null als Nenner auszuschließen ist, ist nun nach Kap. I. § 4 ein orthoider Bereich, den wir mit Kronecker Rationalitätsbereich der Größen $\mathfrak{R}$ nennen und mit

$$(\mathfrak{R}_1 \ldots, \mathfrak{R}_\mu)$$

bezeichnen.

Dabei sind selbstverständlich die Größen $\sum_g k_g \mathfrak{R}_1^{a_1} \mathfrak{R}_2^{a_2} \ldots$ als Größen des ursprünglich vorgelegten orthoiden Bereichs anzusehen, und es ist nicht ausgeschlossen, daß zwei solche Größen gleich werden, ohne daß die entsprechenden Koeffizienten gleich sind. Dies hindert die gegebenen Festsetzungen nicht, wohl aber wird es gut sein, zu beachten, daß die als Nenner ausgeschlossenen Ausdrücke $\sum_{(g)} k_g \mathfrak{R}_1^{a_1} \mathfrak{R}_2^{a_2} \ldots$ diejenigen sind, die als Größen des ursprünglichen Bereichs gleich 0 sind.

Ist nur eine Größe $\mathfrak{R}$ gegeben und diese gleich Eins, so ist der so definierte Rationalitätsbereich der Bereich der rationalen Zahlen, der absolute Rationalitätsbereich, (1).

Sind die Größen $\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu$ durchweg Unbestimmte, $\mathfrak{R}_i = x_i$, so erhält man den dem holoiden Formenbereiche $[[1], x_1, \ldots x_\mu]$ entsprechenden orthoiden Bereich, der als natürlicher Rationalitätsbereich mit den μ Unbestimmten $x_1, \ldots, x_\mu$ in unsrer Zeichensprache kurz mit

$$(x_1, x_2, \ldots x_\mu)$$

bezeichnet wird. Dann können wir den folgenden grundlegenden Kroneckerschen Satz beweisen:

Jeder Rationalitätsbereich ist, insofern nur die in der Theorie der algebraischen Größen untersuchten Eigenschaften in Betracht kommen, d. h. insofern nur die für den ursprünglichen holoiden oder orthoiden Bereich definierten Verknüpfungen in die Fragestellung eintreten, identisch mit einem bestimmten, einem natürlichen Rationalitätsbereiche entstammenden Gattungsbereiche.

Zum Beweise betrachten wir zuerst den in $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$

jedenfalls enthaltenen Rationalitätsbereich $(\mathfrak{R}_1)$. Dann sind zwei Fälle möglich. Die als rationale und ganze Formen von $\mathfrak{R}_1$ definierten Größen

$$\sum_{i=0}^{n} c_i \mathfrak{R}_1^i \qquad (n = 0, 1, \ldots.)$$

sind durchweg von 0 verschieden, wenn nicht alle c_i gleich 0 sind; oder es gibt eine solche Größe, die gleich 0 wird, ohne daß alle Koeffizienten verschwinden.

Im ersten Falle ist der Rationalitätsbereich $(\mathfrak{R}_1)$ in allen seinen Eigenschaften mit dem natürlichen Rationalitätsbereich (x_1) identisch, und $\mathfrak{R}_1$ kann einfach als Zeichen einer Unbestimmten angesehen werden.

Im zweiten Falle hat man für ein bestimmtes n und ein bestimmtes rationales und ganzes Wertsystem $c_0, \ldots, c_n$:

$$\sum_{i=0}^{n} c_i \mathfrak{R}_1^i = 0;$$

zerlegt man die links stehende Form als rationale und ganze Form der Unbestimmten $\mathfrak{R}_1$ in irreduzible Faktoren, so muß einer von ihnen gleich 0 werden, d. h. $\mathfrak{R}_1$ ist eine algebraische Zahl und $(\mathfrak{R}_1)$ ein dem absoluten Rationalitätsbereich entstammender Gattungsbereich.

Ein natürlicher Rationalitätsbereich ist jedoch nichts anderes als der diesem entstammende Gattungsbereich erster Ordnung, also der ausgesprochene Satz für eine Größe $\mathfrak{R}_1$ erwiesen.

Der allgemeine Beweis ergibt sich leicht durch vollständige Induktion. Es kann allgemein angenommen werden, daß der Rationalitätsbereich $(\mathfrak{R}_1, \ldots, \mathfrak{R}_{\mu-1})$ ein Gattungsbereich ist, der einem natürlichen Rationalitätsbereiche entstammt. Es ist demnach auch $(\mathfrak{R}_1, \ldots, \mathfrak{R}_{\mu-1})$ ein orthoider Bereich.

Nun sind wieder nur die beiden Fälle möglich, daß die Formen

$$\sum_{i=1}^{n} \varrho_i \mathfrak{R}_\mu^i \qquad (n = 0, 1, \ldots),$$

in denen $\varrho_0, \ldots, \varrho_n$ dem Rationalitätsbereiche $(\mathfrak{R}_1, \ldots, \mathfrak{R}_{\mu-1})$ angehörige Größen sind, entweder durchweg von 0 verschieden sind, wenn diese Größen nicht sämtlich verschwinden, oder aber für ein bestimmtes n und ein bestimmtes Wertsystem $\varrho_0, \cdots, \varrho_n$

$$\sum_{i=1}^{n} \varrho_i \mathfrak{R}_\mu^i = 0$$

wird.

Im ersten Falle ist $\mathfrak{R}_\mu$ für alle in Betracht kommenden Verknüpfungen nichts anderes als eine neue Unbestimmte, und $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$ wieder ein Gattungsbereich, dessen Stammbereich einfach durch die Unbestimmte $\mathfrak{R}_\mu$ erweitert wurde; denn daß in der die Gleichung definierenden irreduzibeln Gleichung die Koeffizienten die Unbestimmte $\mathfrak{R}_\mu$ nicht enthalten, ist ein spezieller Umstand, der an der Definition des Gattungsbereiches nichts Wesentliches ändert.

Im zweiten Falle ist $\mathfrak{R}_\mu$ wieder Wurzel einer irreduzibeln Gleichung, deren Koeffizienten dem Gattungsbereiche $(\mathfrak{R}_1, \ldots, \mathfrak{R}_{\mu-1})$ angehören, der selbst einem natürlichen Rationalitätsbereiche entstammt; also $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$ ein Gattungsbereich, dessen Stammbereich $(\mathfrak{R}_1, \ldots, \mathfrak{R}_{\mu-1})$ ist. Dann ist aber nach dem in § 18 bewiesenen Satze $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$ in der Tat ein Gattungsbereich, der einem natürlichen Rationalitätsbereiche entstammt.

Insofern die Größen $\mathfrak{R}$ durch „algebraische" Eigenschaften gegeben sind, können diese nichts anderes sein als Gleichungen, denen die Größen $\mathfrak{R}$ genügen, und zwar so, daß die Koeffizienten der Gleichung für $\mathfrak{R}_i$ dem Rationalitätsbereiche $(\mathfrak{R}_1, \ldots, \mathfrak{R}_{i-1})$ angehören; die Unterscheidung der beiden Fälle ergibt sich dann von selbst, damit also auch die Aufstellung des Gattungsbereiches $\mathfrak{G}$, der mit dem gegebenen Rationalitätsbereiche für jede arithmetisch-algebraische Fragestellung als identisch anzusehen ist.

§ 21. Das hiermit für die Theorie der algebraischen Größen gewonnene bedeutungsvolle Resultat soll zuerst in folgenden, der Kroneckerschen Festschrift*) entnommenen Worten charakterisiert werden:

„Die Wahl der Größen $\mathfrak{R}_1, \mathfrak{R}_2, \mathfrak{R}_3 \ldots$, d. h. also der Elemente eines Rationalitäts-Bereichs, unterliegt an sich keinerlei Beschränkung, doch ist es für die Behandlung der algebraischen Größen völlig bedeutungslos, transcendente Zahlengrößen oder transcendente Funktionen von Variabeln unter die Elemente mit aufzunehmen; denn die Resultate bleiben ungeändert, wenn an Stelle solcher transcendenten neue unabhängige Veränderliche gesetzt werden. Sind nämlich die Resultate der Theorie algebraischer Funktionen von $\mathfrak{R}_1, \mathfrak{R}_2, \mathfrak{R}_3 \ldots$ erst für diesen Fall, wo die transcendenten $\mathfrak{R}$ durch unabhängige Variable ersetzt sind, entwickelt, so können dieselben, ihrer Natur und Herleitung nach, nur durch solche Specialisation von Größen $\mathfrak{R}$ alteriert oder modifiziert werden, bei welcher algebraische Beziehungen zwischen denselben eintreten."

Hieraus folgt nun weiter — nach dem eben bewiesenen Satze — und abermals mit den Worten Kroneckers**):

„Man kann sich hiernach schließlich auf die Annahme solcher Rationalitätsbereiche beschränken, in welchen die Elemente eine Anzahl veränderlicher oder unbestimmter Größen sind, zu denen höchstens eine algebraische Funktion derselben tritt. Für ein solches Hinzutreten von Größen $\mathfrak{R}$, die den Rationalitätsbereich in einer für die algebraische Betrachtung wesentlichen Weise modifizieren, bedient man sich seit Galois des technischen Ausdrucks der Adjunktion. Die allgemeinste Annahme kann also dahin formuliert werden, daß für die Größen $\mathfrak{R}$ eine Anzahl Variabler zu setzen und denselben höchstens eine algebraische Funktion zu adjungieren ist. Hierin ist auch der Fall inbegriffen, wo die Größen $\mathfrak{R}$ überhaupt fehlen."

---

*) Beginn des § 3.

**) l. c. § 3. Zweiter Absatz.

Damit ist also die Theorie der algebraischen Größen auf eine Theorie der in Bezug auf $[[1], x_1, \ldots, x_m]$ algebraischen Größen, d. h. der absolut algebraischen Größen reduziert. (S. § 7 dieses Kapitels.)

Wie sich diese Reduktion insbesondere für die durch eine beliebige Gleichung

$$F(z) = 0$$

definierten Größen stellt, soll noch ausführlicher dargelegt werden.

Die Koeffizienten der Form F gehören jedenfalls einem bestimmten Rationalitätsbereiche an, als dessen Elemente im äußersten Falle jene Koeffizienten selbst angesehen werden können. Dieser Rationalitätsbereich ist ein Gattungsbereich, der durch eine Gleichung

$$G(x, \mathfrak{R}_1, \mathfrak{R}_2, \ldots) = 0$$

vollständig definiert wird, wo $\mathfrak{R}_1, \mathfrak{R}_2, \ldots$ Unbestimmte bedeuten, die in die Koeffizienten der Gleichung $G = 0$ eingehen. Bildet man nun den der Gleichung $G = 0$ entsprechenden Galoisschen Bereich, in welchem $\gamma_1, \ldots, \gamma_n$ die Wurzeln der Gleichung sind, so können die Koeffizienten der Gleichung $F = 0$ als rationale und ganze Formen von $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \gamma_i$ geschrieben werden. Sei die so geschriebene Gleichung $F_i(z) = 0$, so wird jede Wurzel der Gleichung auch eine Wurzel von

$$\prod_{i=1}^{n} F_i(z) = 0$$

sein, d. h. durch eine Gleichung definiert sein, deren Koeffizienten dem natürlichen Rationalitätsbereiche $(\mathfrak{R}_1, \mathfrak{R}_2, \ldots)$ angehören.

Auf Größen, die als Wurzeln irgend welchen Gleichungssystems definiert sind, läßt sich nach den in Kap. III. § 20 gegebenen Entwicklungen diese Erörterung ebenfalls unmittelbar übertragen; doch möge dies für eine spätere Stelle (Kap. V, § 7) vorbehalten bleiben, wo die Eliminationsprobleme in ihrem inneren Zusammenhange darzulegen sein werden.

Sind die Größen eines orthoiden Bereichs nicht durch algebraische Methoden, sondern durch anderweitige Begriffsbildungen bestimmt, hat man es z. B. mit sogenannten Grenzwerten der Analysis zu tun, so liegt die Frage, ob ein solcher Grenzwert eine algebraische Größe darstellt, gänzlich außerhalb der Sphäre algebraischer Methoden. Diese Fragestellung führt zu den schwierigsten Problemen der Mathematik; so ist erst in neuerer Zeit der „transcendente" d. h. nicht algebraische Charakter der mit e und π bezeichneten Grenzwerte von Hermite (1873) und Lindemann (1882) festgestellt worden.

Ist einmal der transcendente Charakter einer Zahl wie e festgestellt, so wird diese in jedem Gleichungssysteme genau wie eine Unbestimmte zu behandeln sein; würde aber in einem solchen e und π vorkommen, so ist es immer noch fraglich, ob π nicht mit e „algebraisch verbunden" ist, d. h. nicht vielleicht eine Gleichung mit ganzzahligen Koeffizienten $\sum_{r=0}^{m} \sum_{s=0}^{n} k_{rs} e^r \pi^s = 0$ existiert?

§ 22. Ist $(\mathfrak{R}_1, \ldots, \mathfrak{R}_\mu)$ irgend ein Rationalitätsbereich, so können seine sämtlichen Größen auf die Gestalt

$$r_0 \omega_0 + r_1 \omega_1 + \cdots + r_{n-1} \omega_{n-1}$$

gebracht werden, wo die r_i einem natürlichen Rationalitätsbereiche $(x_1, \ldots, x_m)$ angehören. Dazu hat man nur für die $x_1, \ldots, x_m$ jene Größen $\mathfrak{R}$ zu nehmen, die als Unbestimmte verbleiben, wenn man den Rationalitätsbereich als Gattungsbereich auffaßt, und $\omega_i = \gamma^i$ zu setzen, wenn dieser Gattungsbereich durch die der irreduzibeln Gleichung n^{ten} Grades

$$F(z; x_1, \ldots, x_m) = 0$$

genügende Größe γ definiert ist.

Daß ein solches System von Werten $\omega_0, \omega_1, \ldots, \omega_{n-1}$ auf unendlich viele verschiedene Weisen gewählt werden kann, ist unmittelbar einzusehen; denn, wenn man z. B.

$$\omega_h = \sum_{k=0}^{n-1} r_{hk} \gamma^k \qquad (h = 0, 1, \ldots, n-1)$$

setzt, wird $\omega_0, \omega_1, \ldots, \omega_{n-1}$ immer ein solches System sein, wenn die Größen r_{hk} dem natürlichen Rationalitätsbereiche $(x_1, \ldots, x_m)$ angehören und ihre Determinante $|r_{hk}|$ von 0 verschieden ist.

Diese Darstellung wird in der Folge fortwährend gebraucht werden und ist deshalb von besonderer Wichtigkeit, weil sie für Rationalitätsbereiche charakteristisch ist, d. h. die folgende Umkehrung gestattet:

Wenn sämtliche Größen eines orthoiden Bereichs in der Form

$$r_0 \omega_0 + \cdots + r_{n-1} \omega_{n-1}$$

darstellbar sind, wo die r einem natürlichen Rationalitätsbereiche angehören, so ist der orthoide Bereich ein Rationalitätsbereich.

Ist nämlich ω eine beliebige Größe des orthoiden Bereichs, so ist der Annahme nach

$$\omega \omega_h = \sum_{k=0}^{n-1} r_{hk} \omega_k, \qquad (h = 0, \ldots, n-1)$$

ein Gleichungssystem, das auch in der Gestalt

$$\sum_{k=0}^{n-1} (r_{hk} - \delta_{hk} \omega) \omega_k = 0 \qquad (h = 0, \ldots, n-1)$$

geschrieben werden kann, wenn, wie bei früheren Anlässen, $\delta_{hh} = 1$ und $\delta_{hk} = 0 \,(h \neq k)$ ist. Da der orthoide Bereich auch die Eins enthält und demnach die Größen ω_k nicht sämtlich verschwinden, muß die Determinante

$$|r_{hk} - \delta_{hk} \omega| = 0$$

sein, d. h. die Größe ω einer Gleichung genügen, deren Koeffizienten dem natürlichen Rationalitätsbereiche $(x_1, \ldots, x_m)$ angehören. Dies ist insbesondere auch für die Größen

$$\omega_0, \omega_1, \ldots, \omega_{n-1}$$

der Fall. Der orthoide Bereich ist also mit dem Rationalitätsbereiche $(x_1, \ldots, x_m, \omega_0, \ldots, \omega_{n-1})$ identisch.

Dabei ergibt sich gleichzeitig, wie die Anzahl der Elemente in $\omega_0, \ldots, \omega_{n-1}$ auf die notwendige kleinste Zahl beschränkt werden kann. Denn, wenn der Rationalitätsbereich als dem natürlichen Rationalitätsbereiche $(x_1, \ldots, x_m)$ entstammender Gattungsbereich von der s^{ten} Ordnung ist, so gibt es ein System

$$\omega_i = \gamma^i \qquad (i = 0, 1, \ldots, s-1),$$

das schon den Forderungen entspricht, und keines, das weniger Elemente enthält.

Der erste Teil des Satzes ist nach den Eingangsworten dieses Paragraphen evident. Gäbe es aber ein entsprechendes System $\omega_0', \ldots, \omega_{r-1}'$, wo $r < s$ wäre, so müßte jede Größe des Bereichs einer Gleichung vom Grade r mit Koeffizienten aus $(x_1, \ldots, x_m)$ genügen, während doch γ eine Größe des Bereichs ist, die einer solchen irreduzibeln Gleichung s^{ten} Grades $(s > r)$ genügt, also keiner ähnlichen Gleichung r^{ten} Grades genügen kann.

Die notwendige kleinste Anzahl der Elemente in $\omega_0, \omega_1, \ldots, \omega_{n-1}$ ist also nichts anderes als die Ordnung des Rationalitätsbereichs, wenn man diesen als einem natürlichen Rationalitätsbereiche entstammenden Gattungsbereich auffaßt.

Jedes solche Wertsystem $\omega_0, \omega_1, \ldots$, das auf die kleinste Anzahl der Elemente gebracht ist, heißt eine Basis*) des Rationalitätsbereichs. Damit erhält der Ausdruck „Rationalitätsbereich“ eine neue, tiefere Bedeutung. Man kann nämlich unmittelbar die Größen desselben als Komplexe von — im absoluten Sinne des Wortes — rationalen Größen $(r_0, r_1, \ldots, r_{n-1})$ deuten, deren Zusammenfassung in einen orthoiden Bereich durch Verknüpfungen stattfindet, die ausschließlich an diesen Komplexen statuiert werden, wenn sie sich auch kürzer und bequemer an die Schreibweise

*) Dirichlet-Dedekind, Zahlentheorie, IV. Aufl. pag. 468.

$r_0\omega_0 + \cdots + r_{n-1}\omega_{n-1}$ anschließen. Und damit reduziert sich prinzipiell die Theorie der algebraischen Größen auf eine Theorie der einem natürlichen Rationalitätsbereiche angehörigen Größenkomplexe.

Dem Gesagten gegenüber muß aber auch bemerkt werden, daß der Zusammenfassung algebraischer Größen in Rationalitätsbereiche dadurch Grenzen gesteckt sind, daß jene Größenkomplexe aus einer bestimmten endlichen, wenn auch noch so großen Anzahl von Elementen bestehen. So bildet die Gesamtheit der algebraischen Zahlen wohl einen orthoiden Bereich, aber keinen Rationalitätsbereich mehr. Wäre letzteres der Fall, so müßte er als Gattungsbereich von einer bestimmten Ordnung n sein, und jede algebraische Zahl würde einer Gleichung mit rationalen und ganzen Koeffizienten genügen, deren Grad ein Teiler von n ist. Nun gibt es aber algebraische Zahlen, die durch eine irreduzible Gleichung vom beliebig hohen Grade N definiert werden (§ 4 dieses Kap.), womit die obige Behauptung erwiesen ist.

Der Begriff des orthoiden Bereichs ist hiernach viel weiter als der des Rationalitätsbereichs; er wird auch noch durch Begriffsbildungen, wie es das Reich der algebraischen Zahlen oder algebraischen Funktionen sind, nicht erschöpft. Die in der Analysis betrachteten Gesamtheiten der reellen oder auch der komplexen Zahlen sind orthoide Bereiche.

Hier wird es auch angezeigt sein, den von Dedekind eingeführten Ausdruck „Körper“ zu erwähnen, der vielfach fälschlich als mit dem Kroneckerschen Rationalitätsbereich gleichbedeutend angesehen wird.

„Ein System A von reellen oder komplexen Zahlen a soll“ — nach der Dedekindschen Definition*) — „ein Körper heißen, wenn die Summen, Differenzen, Produkte und Quotienten von je zwei dieser Zahlen a demselben System A angehören.“

Abgesehen von der wohl von Dedekind als selbstverständlich angesehenen Beziehung auf ein „gewöhnliches“ Additions-

*) l. c. pag. 452.

und Multiplikationsgesetz ist die Definition des „Körpers“ im wesentlichen, wenn auch mit gewissen methodischen Unterschieden, die des orthoiden Bereichs. Daß ich dennoch diesen neuen Ausdruck wählen mußte, war eine notwendige Folge des für einen systematischen Aufbau der Theorie unvermeidlichen Umstandes, daß der holoide und orthoide Bereich von Anfang an prinzipiell einander gegenüberzustellen waren und daß es in dieser parallelen Benennung am klarsten erscheint, wie in deren Definition die wesentlichen Eigenschaften des Bereichs der rationalen und ganzen Zahlen, resp. der rationalen Zahlen, und nur diese aufgenommen werden. Außerdem war noch der Einklang mit der weiteren, konsequent ausgebildeten Kroneckerschen Terminologie zu berücksichtigen.

Das Galoissche Prinzip.

§ 23. Es sei $F(z) = 0$ eine Gleichung n^{ten} Grades, deren Koeffizienten einem beliebigen Rationalitätsbereiche angehören und deren Discriminante von Null verschieden ist. Ihre Wurzeln in dem durch entsprechende Adjunktion entstandenen Galoisschen Bereiche seien $\xi_1, \ldots, \xi_n$, der Voraussetzung nach sind dann $\xi_1, \ldots, \xi_n$ n verschiedene Größen dieses Bereichs.

Bildet man das über alle Permutationen $i_1, \ldots, i_n$ der Zahlen $1, \ldots, n$ erstreckte Produkt

$$\prod_{(i)} (x - u_1 \xi_{i_1} - u_2 \xi_{i_2} - \ldots - u_n \xi_{i_n}),$$

so ist dieses eine symmetrische Form der Größen $\xi_1, \ldots, \xi_n$, also eine solche Form der Unbestimmten $x, u_1, \ldots, u_n$, deren Koeffizienten dem vorgelegten Rationalitätsbereiche angehören. Als solche in irreduzible Faktoren zerlegt, sei diese:

$$G(x; u_1, \ldots, u_n) = G_1(x; u_1, \ldots, u_n)\, G_2(x; u_1, \ldots, u_n) \ldots$$

Der bloße Anblick lehrt, daß das über alle Permutationen $j_1, \ldots, j_n$ der Zahlen $1, \ldots, n$ erstreckte Produkt

$$\prod_{(j)} (x - u_{j_1} \xi_1 - u_{j_2} \xi_2 - \ldots - u_{j_n} \xi_n)$$

mit dem früher hingeschriebenen identisch ist; daß also $G(x; u_1, \ldots, u_n)$ auch eine symmetrische Form der Unbestimmten $u_1, \ldots, u_n$ ist. Dann wird auch

$$\underline{G}(x; u_{r_1}, \ldots, u_{r_n}) = G_1(x; u_{r_1}, \ldots, u_{r_n})\, G_2(x; u_{r_1} \ldots, u_{r_n}) \ldots$$
$$= G(x; u_{s_1}, \ldots, u_{s_n}) = G_1(x; u_{s_1}, \ldots, u_{s_n})\, G_2(x; u_{s_1}, \ldots, u_{s_n}) \ldots,$$

und die Produkte rechts ergeben wieder die Zerlegung in irreduzible Faktoren, da sie sich von $G_1(x; u_1, \ldots, u_n), \ldots$ ja nur in der Benennung der Unbestimmten unterscheiden. Die Faktoren $G_1, G_2, \ldots$ sind übrigens nach § 12 von gleicher Dimension.

Es seien nun

$$x - u_{r_1}\xi_1 - u_{r_2}\xi_2 - \ldots - u_{r_n}\xi_n$$
$$x - u_{s_1}\xi_1 - u_{s_2}\xi_2 - \ldots - u_{s_n}\xi_n$$
$$\ldots\ldots\ldots\ldots\ldots$$

irgend welche linearen Faktoren, die demselben im ursprünglichen Rationalitätsbereiche irreduzibeln Faktor, z. B. G_1 angehören. (Der Grenzfall, wo die Faktoren $G_1, \ldots$ sämtlich von der Dimension Eins sind, wird später leicht zu erledigen sein.) Dann wird:

$$G_1(x; u_{r_1}, \ldots, u_{r_n}) = G_1(x; u_{s_1}, \ldots, u_{s_n}) = \ldots, \qquad (1)$$

denn die Resultante je zweier ist Null, während diese doch irreduzibel sind und ihr höchstes Glied (in x) übereinstimmt.

Es gibt daher, wenn die Dimension von G_1 z. B. k ist, k Permutationen der Größen $u_1, \ldots, u_n$

$$u_{r_1}, \ldots, u_{r_n},$$
$$u_{s_1}, \ldots, u_{s_n}, \qquad (P)$$
$$\ldots\ldots,$$

„für welche die Form G_1 sich nicht ändert“. So möge nämlich die in (1) ausführlich definierte Eigenschaft kurz ausgedrückt werden. Wenn man in einer Form $F(u_1, \ldots, u_n)$ an Stelle von $u_{r_1}, \ldots, u_{r_n}$ der Reihe nach $u_{s_1}, \ldots, u_{s_n}$ setzt, so ist dies eine bestimmte, leicht ausführbare „Operation“ an der Form F, die Substitution genannt wird und mit

$$S_{rs} = \begin{pmatrix} u_{r_1}, \ldots, u_{r_n} \\ u_{s_1}, \ldots, u_{s_n} \end{pmatrix}$$

bezeichnet werden kann. Wenn man die Substitution S_{rs} an F ausführt, ist das Resultat eine neue Form, die kurz $S_{rs}F$ geschrieben werden möge. Ist nun

$$S_{st} = \begin{pmatrix} u_{s_1}, \ldots, u_{s_n} \\ u_{t_1}, \ldots, u_{t_n} \end{pmatrix}$$

eine zweite Substitution, so können beide auch nacheinander, d. h. an der Form $S_{rs}F$ wieder die Substitution S_{st} ausgeführt werden; und es ist klar, daß die hierdurch bewirkte Änderung in F auch auf einmal durch die eine Substitution

$$S_{rt} = \begin{pmatrix} u_{r_1}, \ldots, u_{r_n} \\ u_{t_1}, \ldots, u_{t_n} \end{pmatrix}$$

ausgedrückt werden kann. Man schreibt demgemäß

$$S_{rt} = S_{st} S_{rs},$$

wo die rechts stehenden Substitutionen in der Reihenfolge von rechts nach links auszuführen sind. Die Bedeutung dieser symbolischen Gleichung ist einfach die, daß für jede Form $F(u_1, \ldots, u_n)$

$$S_{rt}F = S_{st}(S_{rs}F)$$

wird. Dabei bezeichnet man $S_{st}S_{rs}$ als Folge oder auch als Produkt der Substitutionen S_{st} und S_{rs}. Bei Benutzung des allgemein gebräuchlichen Ausdrucks „Produkt" ist jedoch darauf zu achten, daß die Reihenfolge der Faktoren im allgemeinen nicht vertauscht werden darf.

Jene Eigenschaft der Form G_1 kann demnach auch so ausgedrückt werden, daß diese sich bei keiner der Substitutionen S_{rs} ändert, die aus den Permutationen (P) entstehn, wenn man in dem für Substitutionen eingeführten Symbole irgend zwei dieser Permutationen als erste und zweite Zeile benutzt. Diese Substitutionen bilden eine Gruppe, ein Ausdruck, mit dem wir kurz diejenige Eigenschaft dieser

Reihe von Substitutionen bezeichnen, daß das Produkt von irgend zwei dieser Substitutionen wieder in der Reihe enthalten ist. Das wird aus der Bemerkung evident, daß ein solches Produkt jedenfalls eine solche Substitution liefert, die G_1 nicht ändert, während andrerseits jede Substitution, die G_1 nicht ändert, in der Reihe enthalten sein muß. Auch das ist sehr einfach nachzuweisen, denn, damit es der Fall sei, muß ein linearer Faktor $x - u_{r_1}\xi_1 - \cdots - u_{r_n}\xi_n$ bei dieser Substitution in einen andern linearen Faktor von G_1, also z. B. $x - u_{s_1}\xi_1 - \cdots - u_{s_n}\xi_n$ übergehn, und die Substitution muß daher die Gestalt S_{rs} besitzen.

Dem entsprechend sagen wir auch, daß die Permutationen (P) eine Gruppe bilden.

Diese Entwicklung führt also zu einer dem gegebenen Rationalitätsbereiche entstammenden Form

$$G_1(x; u_1, \ldots, u_n),$$

die sich für die Gruppe der Substitutionen S_{rs} und nur für diese nicht ändert.

Man kann nun weiter für x in G_1 beliebig viele dem ursprünglichen Rationalitätsbereiche angehörige Größen, auch rationale und ganze Zahlen a setzen, so daß die spezielle Form

$$G_1(a; u_1, \ldots, u_n) = \Gamma_1(u_1, \ldots, u_n)$$

genau dieselbe Eigenschaft besitzt. Daß sich Γ_1 für die Substitutionen nicht ändert, wenn es sich für G_1 ebenso verhält, ist unmittelbar klar. Wäre aber für irgend eine Substitution S_{rs}:

$$S_{rs}\Gamma_1 = \Gamma_1,$$

ohne daß

$$S_{rs}G_1 = G_1$$

ist, so wäre $S_{rs}G_1 - G_1$ eine Form der u, deren Koeffizienten, als ganze Funktionen von x aufgefaßt, nicht sämtlich verschwinden. Da die Anzahl der Substitutionen eine bestimmte, endliche ist, kann man solche Werte a für x bestimmen, daß

auch $S_{rs}\Gamma_1 - \Gamma_1$ nur dann von 0 verschieden ist, wenn das für $S_{rs}G_1 - G_1$ der Fall ist. Damit ist aber unsre Behauptung erwiesen.

§ 24. Jeder lineare Faktor von Γ_1:

$$L = a - u_{t_1}\xi_1 - u_{t_2}\xi_2 - \cdots - u_{t_n}\xi_n$$

kann auch in einer der beiden Gestalten

$$a - u_{r_1}\xi_{\varrho_1} - u_{r_2}\xi_{\varrho_2} - \cdots - u_{r_n}\xi_{\varrho_n}$$

oder

$$a - u_{s_1}\xi_{\sigma_1} - u_{s_2}\xi_{\sigma_2} - \cdots - u_{s_n}\xi_{\sigma_n}$$

geschrieben werden, und die in den Unbestimmten u ausgeführte Substitution S_{rs} gibt

$$S_{rs}L = a - u_{s_1}\xi_{\varrho_1} - u_{s_2}\xi_{\varrho_2} - \cdots - u_{s_n}\xi_{\varrho_n}.$$

Die an den Größen ξ ausgeführten Substitutionen können ähnlich bezeichnet werden. Es sei

$$\Sigma_{\varrho\sigma} = \begin{pmatrix} \xi_{\varrho_1}, & \xi_{\varrho_2}, & \cdots, & \xi_{\varrho_n} \\ \xi_{\sigma_1}, & \xi_{\sigma_2}, & \cdots, & \xi_{\sigma_n} \end{pmatrix}.$$

Dann ist ebenso

$$\Sigma_{\sigma\varrho} = \begin{pmatrix} \xi_{\sigma_1}, & \xi_{\sigma_2}, & \cdots, & \xi_{\sigma_n} \\ \xi_{\varrho_1}, & \xi_{\varrho_2}, & \cdots, & \xi_{\varrho_n} \end{pmatrix},$$

und $\Sigma_{\sigma\varrho}\Sigma_{\varrho\sigma}$ augenscheinlich eine identische Substitution, die jedes Element an seiner Stelle beläßt. Dieses Verhalten der beiden (inversen) Substitutionen wird zweckmäßig durch die symbolische Gleichung

$$\Sigma_{\sigma\varrho}\Sigma_{\varrho\sigma} = 1$$

charakterisiert. Man hat bei diesen Bezeichnungen

$$\Sigma_{\varrho\sigma}S_{rs}L = L$$

oder, wenn man auf beiden Seiten noch die Substitution $\Sigma_{\sigma\varrho}$ ausübt,

$$S_{rs}L = \Sigma_{\sigma\varrho}L = L.$$

Die an Γ_1 durch Substitutionen der u bewirkten Änderungen können also auch durch Substitutionen der ξ bewirkt werden und umgekehrt, und zwar bestimmen sich diese Substitutionen gegenseitig eindeutig. Dem Produkt zweier S entspricht das Produkt der entsprechenden Σ, der Gruppe der S die Gruppe der Σ.

Die Form Γ_1 bleibt daher ungeändert für alle Substitutionen $\Sigma_{\varrho\sigma}$, ... und nur für diese. Diese Substitutionen bilden eine Gruppe: ihre Anzahl ist ebenso groß wie die der Gruppe S_{rs}.

Die Ordnung einer Gruppe ist die Anzahl der in ihr enthaltenen Substitutionen, wobei die „identische" Substitution stets mitzuzählen ist.

Die Gruppe der Substitutionen S_{rs} und auch der Substitutionen $\Sigma_{\sigma\varrho}$ ist demnach von der Ordnung k, und k ist die Dimension von G_1 oder die Anzahl der Permutationen in (P). Denn es gibt eine Substitution, die einen bestimmten linearen Faktor in einen beliebigen zweiten überführt, und nur eine solche, da die Substitution hierdurch vollständig bestimmt ist; es gibt also ebensoviele Substitutionen in der Gruppe, als Permutationen in (P) vorhanden sind.

Man kann schließlich, wenn man Γ_1, um das Auftreten der ξ zu charakterisieren, jetzt $\Gamma_1(u_1, \ldots, u_n, \xi_1, \ldots, \xi_n)$ schreibt, wieder statt $u_1, \ldots, u_n$ Größen des Rationalitätsbereichs, auch rationale und ganze Zahlen setzen, so daß auch $\Gamma_1(a_1, \ldots, a_n, \xi_1, \ldots, \xi_n)$ sich bei den Substitutionen $\Sigma_{\sigma\varrho}$ und nur bei diesen nicht ändert. Der Beweis wird genau mit denselben Worten geführt, wie am Schlusse des vorhergehenden Paragraphen.

Für jede Gleichung, die einem bestimmten Rationalitätsbereiche angehörige Koeffizienten besitzt, gibt es eine bestimmte „charakteristische" Gruppe von Substitutionen, als deren Elemente die Unbestimmten u oder auch die Wurzeln ξ der Gleichung auftreten; wir besitzen ferner eine Methode zur Bildung bestimmter Formen sowohl der Unbestimmten u wie

der Wurzeln ξ, deren Koeffizienten dem Rationalitätsbereiche angehören und die sich für die der charakteristischen Gruppe angehörigen Substitutionen und nur für diese nicht ändern.

Der so ausgesprochene Satz ist das Galoissche Prinzip der Theorie der algebraischen Gleichungen*), das erst zur vollen Erkenntnis der in dieser Theorie auftretenden Probleme und Methoden geführt hat. Die Fassung des Satzes in Bezug auf die Wurzeln ξ ist die ursprünglich von Galois gegebene; die Formulierung, die nur die Unbestimmten u in Anspruch nimmt und dadurch den Satz vollständig in die Theorie der einem Rationalitätsbereich entstammenden Formen einbezieht, rührt von Kronecker her.

§ 25. Jene im Ausspruch des Galoisschen Prinzips definierte Gruppe von Substitutionen $\Sigma_{\varrho\sigma}$ wird für die Theorie der Gleichung $F(z) = 0$ durch folgende Tatsache von grundlegender Bedeutung.

Ist φ irgend eine dem vorgelegten Rationalitätsbereiche entstammende Form gewisser Unbestimmter und der Wurzeln $\xi_1, \ldots, \xi_n$, d. h. eine Größe von der Gestalt

$$\varphi = \sum_{(k)} c_k \xi_1^{k_1} \xi_2^{k_2} \ldots \xi_n^{k_n},$$

wo die c_k dem Rationalitätsbereiche entstammende Formen sind, so wird die Größe φ dann und nur dann eine dem Rationalitätsbereiche entstammende Form sein, wenn sie sich für die Gruppe der Substitutionen $\Sigma_{\varrho\sigma}$ nicht ändert.

Bildet man die Galoissche Resolvente von $F(z) = 0$ im Sinne des § 11 dieses Kapitels, indem man die u als Unbestimmte beläßt und jenen irreduzibeln Faktor wählt, welcher den linearen Faktor $x - u_1 \xi_{\varrho_1} - \cdots - u_n \xi_{\varrho_n}$ enthält, so ist

*) Kronecker, Festschrift. § 11.

für die auf der linken Seite dieser Gleichung stehende Form

$$G_1(x, u, \ldots, u_n) = \Pi(x - u_1\xi_{i_1} - \cdots - u_n\xi_{i_n}),$$

wo sich das Produktzeichen auf alle Permutationen erstreckt, die aus $\varrho_1, \ldots, \varrho_n$ durch die Gruppe der Substitutionen $\Sigma_{\varrho\sigma}$ entstehen. Dabei bleibt G_1 nur für die Substitutionen dieser Gruppe ungeändert; denn jede andere Substitution führt zum mindesten einen linearen Faktor ein, der in einem andern irreduzibeln Faktor von G enthalten ist.

Ist nun φ für die Gruppe der Substitutionen $\Sigma_{\varrho\sigma}$ unveränderlich, also

$$\varphi(\xi_{\varrho_1}, \ldots, \xi_{\varrho_n}) = \varphi(\xi_{\sigma_1}, \ldots, \xi_{\sigma_n}) = \ldots,$$

so wird nach § 10 jedenfalls $\xi_{\varrho_1}, \ldots, \xi_{\varrho_n}$, also auch φ in der Gestalt

$$\Theta^l\varphi(\xi_{\varrho_1}, \ldots, \xi_{\varrho_n}) = H(u_1\xi_{\varrho_1} + \cdots + u_n\xi_{\varrho_n}) \qquad (\varphi)$$

identisch darstellbar sein, wo, wie an der citierten Stelle

$$\Theta = \pm \Delta^K U_t + \cdots$$

und $\Delta = \mathrm{Dscr.}\, F$, ferner $H(z)$ eine dem gegebenen Rationalitätsbereich entstammende Form von $z, u_1, \ldots, u_n$ ist. Jene Identität bleibt aber ihrer Entstehung nach gültig, wenn man für $\varrho_1, \ldots, \varrho_n$ irgend eine Permutation setzt, also wird, wenn man über alle Permutationen der Gruppe addiert, da φ der Annahme nach ungeändert bleibt,

$$k\Theta^l\varphi = \sum_{(\varrho)} H(u_1\xi_{\varrho_1} + \cdots + u_n\xi_{\varrho_n}).$$

Die rechts stehende Summe ist aber symmetrisch in den Wurzeln der Galoisschen Resolvente, demnach eine dem Rationalitätsbereiche entstammende Form. Wenn also φ die Unbestimmten $u_1, \ldots, u_n$ nicht enthält, ergibt sich durch Vergleichung der Koeffizienten von U_t in der Tat φ als Größe des Rationalitätsbereichs. Ist aber φ eine Form dieser oder anderer Unbestimmter, so muß jeder Koeffizient eines Potenzproduktes von ihnen bei den Substitutionen $\Sigma_{\varrho\sigma}$ ungeändert bleiben, und φ ist auch dann eine dem Rationalitätsbereiche entstammende Form dieser Unbestimmten.

Wenn umgekehrt φ eine dem Rationalitätsbereiche angehörende Form ist, so ist wegen der Identität (φ)

$$\Theta^l \varphi = H(z)$$

eine Gleichung, welcher die Wurzel $u_1 \xi_{\varrho_1} + \cdots + u_n \xi_{\varrho_n}$ der irreduzibeln Galoisschen Resolvente genügt. Es genügt ihr auch also jede andere Wurzel derselben, und man hat identisch:

$$\Theta^l \varphi = H(u_1 \xi_{\varrho_1} + \cdots + u_n \xi_{\varrho_n}) = H(u_1 \xi_{\sigma_1} + \cdots + u_n \xi_{\sigma_n}) = \cdots,$$

also ändert sich φ für die Gruppe der Substitutionen $\Sigma_{\varrho\sigma}$ nicht; womit der ausgesprochene Satz erwiesen ist. Für jenen Grenzfall, wo die Galoissche Resolvente vom ersten Grade ist, reduziert sich die Gruppe der Substitutionen $\Sigma_{\varrho\sigma}$ auf die einzige identische Substitution, und jede Wurzel der Gleichung $F(z) = 0$ und jede Form φ entstammt dem vorgelegten Rationalitätsbereich.

Der eben bewiesene Satz zeigt unmittelbar, daß es nur eine charakteristische Gruppe von Substitutionen gibt, bei deren Bildung man daher auch von jedem irreduzibeln Teiler der Galoisschen Resolvente ausgehen kann.

§ 26. Als allgemeine Gleichung n^{ten} Grades wird

$$F(z) = z^n + a_1 z^{n-1} + \cdots + a_n = 0$$

bezeichnet, wenn die Koeffizienten $a_1, \ldots, a_n$ durchweg voneinander unabhängige Unbestimmte sind, also die Form F dem natürlichen Rationalitätsbereiche $(a_1, \ldots, a_n)$ entstammt.

Für die allgemeine Gleichung n^{ten} Grades ist die charakteristische Gruppe die allgemeinste, die aus den n Wurzeln $\xi_1, \ldots, \xi_n$ gebildet werden kann, d. h. sie enthält alle Substitutionen, durch welche $\xi_1, \ldots, \xi_n$ in eine beliebige andere Permutation übergeführt werden kann, und ist demnach von der Ordnung $n!$

Um dies nachzuweisen, ist nur zu zeigen, daß, wenn φ eine dem Rationalitätsbereiche $(a_1, \ldots, a_n)$ entstammende Form von $\xi_1, \ldots, \xi_n, v_1, v_2, \ldots$ ist, ohne daß sie symmetrisch in den Wurzeln

ξ ist, φ keine dem Rationalitätsbereiche $(a_1, \ldots, a_n)$ entstammende Form sein kann. Die entgegengesetzte Behauptung ließe sich in der Gestalt

$$A\varphi - B = 0$$

schreiben, wo A und B rationale und ganze Formen von $a_1, \ldots, a_n$ und den eventuell in φ enthaltenen Unbestimmten $v_1, v_2, \ldots$ sind.

Setzt man in $A\varphi - B$ statt $a_1, \ldots, a_n$ die elementaren symmetrischen Formen von $\xi_1, \ldots, \xi_n$, so ist $A\varphi - B$ eine Form der ξ_i, die, insofern man diese als Unbestimmte auffaßt, nicht 0 wird, denn B ist eine symmetrische Form von ihnen, während dies für $A\varphi$ der Annahme nach nicht der Fall ist. Dasselbe bleibt richtig, wenn man für $\xi_1, \ldots, \xi_n$ irgend eine Permutation dieser Größen setzt. Bezeichnet man die so aus φ entstehenden Formen mit $\varphi_1, \varphi_2, \ldots$, so wird auch

$$\Pi(A\varphi_i - B)$$

als Form der ξ_i nicht verschwinden, also auch dann nicht, wenn man die ξ_i durch die a_i ersetzt, was vollständig geschehn kann, da ja jenes Produkt augenscheinlich in den ξ_i symmetrisch ist. Andrerseits muß aber, wegen der Annahme $A\varphi_1 - B = 0$, jenes Produkt gleich Null sein. Man hätte also eine Gleichung

$$\sum_{(g)} k_g A_g = 0,$$

wo die k_g ganze Zahlen bedeuten und die A_g Potenzprodukte der Größen a_i sind; was der Voraussetzung, daß die a unabhängige Unbestimmte sind, widersprechen würde.

Auf den bisher entwickelten Fundamentalsätzen baut sich nun die weittragende Galoissche Theorie der algebraischen Gleichungen auf. Hier sollte nur gezeigt werden, wie diese mit der allgemeinen Theorie der algebraischen Größen in Beziehung tritt; eine Auseinandersetzung der wichtigen speziellen Probleme, die in ihr behandelt werden, liegt außerhalb des Planes dieser Darstellung*).

*) Um so mehr, als für diese Theorie eine Reihe hervorragender Lehrbücher vorliegt, und auch die Kroneckerschen Vorlesungen, deren

Der Gaußsche Fundamentalsatz.

§ 27. Anhangsweise muß noch in diesem Kapitel dargelegt werden, wie die Theorie der algebraischen Größen zu dem s. g. „Fundamentalsatze der Algebra“ in Beziehung tritt. Diese Beziehung wird durch eine Identität vermittelt, die Gauß in einer berühmten Abhandlung*) gegeben hat. Es sei $F(z) = 0$ eine Gleichung n^{ten} Grades, deren Koeffizienten einem beliebig vorgelegten orthoiden Bereiche angehören und deren Discriminante von 0 verschieden ist. Bildet man den entsprechenden Galoisschen Bereich, so hat die Gleichung darin n verschiedene Wurzeln, die mit $\xi_1, \ldots, \xi_n$ bezeichnet werden mögen. Sodann ist

$$u(\xi_i + \xi_j) + v\xi_i\xi_j$$

eine Form von u und v, die bei Vertauschung der ξ_i augenscheinlich $\frac{n(n-1)}{2}$ Werte annimmt, denen ebensoviel Kombinationen (i, j) entsprechen, die aus den Zahlen $1, \ldots, n$ gebildet werden können. Diese Werte sind auch verschieden, denn es kann nur dann

$$u(\xi_i + \xi_j) + v\xi_i\xi_j = u(\xi_{i'} + \xi_{j'}) + v\xi_{i'}\xi_{j'}$$

sein, wenn

$$\xi_i + \xi_j = \xi_{i'} + \xi_{j'}, \quad \xi_i\xi_j = \xi_{i'}\xi_{j'}$$

wird, also auch

$$(z - \xi_i)(z - \xi_j) = (z - \xi_{i'})(z - \xi_{j'})$$

ist. Dazu muß aber das Zahlenpaar (i, j) mit dem Zahlenpaar (i', j') übereinstimmen, was eben ausgeschlossen wurde.

Herausgabe nahe bevorsteht, darauf genauer eingehn. Noch müssen die „Vorlesungen über das Ikosaeder“ und die „Vorlesungen über die Theorie der elliptischen Modulfunktionen“ von Felix Klein erwähnt werden, Werke, die insbesondere die Beziehungen der algebraischen Probleme zu anderen mathematischen Disziplinen betonen und in der elegantesten Form darlegen.

*) Demonstratio nova altera etc. Werke Bd. III. Diese Abhandlung von Gauß war das erste und klassische Muster für die folgerichtige Entwicklung der Theorie der algebraischen Größen.

Das über alle Kombinationen (i, j) ausgedehnte Produkt

$$\prod_{(i,j)}(x - u(\xi_i + \xi_j) - v\xi_i\xi_j)$$

ist daher symmetrisch in den ξ_i und demnach eine dem ursprünglich vorgelegten orthoiden Bereiche entstammende Form der Unbestimmten x, u und v, die mit $G(x, u, v)$ bezeichnet werden möge. Die Gleichung

$$G(x, u, v) = 0$$

vom Grade $\frac{n(n-1)}{2}$ hat demnach die $\frac{n(n-1)}{2}$ Wurzeln

$$u(\xi_i + \xi_j) + v\xi_i\xi_j,$$

die untereinander verschieden sind, und man wird insbesondere an Stelle von u und v auch rationale und ganze Zahlen setzen können, ohne daß sich diese Verhältnisse ändern; denn die Discriminante von G nach x ist eine von 0 verschiedene Form der Unbestimmten u und v, und man hat für u und v nur solche ganze Zahlen zu wählen, für welche aus dieser Form eine von 0 verschiedene Größe entsteht.

Es seien nun a und b zwei so gewählte Zahlen und der Kürze wegen

$$\eta_{ij} = a(\xi_i + \xi_j) + b\xi_i\xi_j;$$

ferner σ_{ij} irgend eine dem orthoiden Bereiche entstammende Form von ξ_i und ξ_j, die in Bezug auf diese beiden Größen symmetrisch ist.

Dann ergibt sich aus dem Gleichungssystem

$$\sigma_{ij} = \sum_{r=0}^{\frac{n(n-1)}{2}-1} \alpha_r \eta_{ij}^r \qquad (\sigma)$$

$$(i, j = 1, 2, \ldots, n;\ i < j)$$

für die Größen α_r:

$$\Delta^2 \alpha_r = \Delta \Delta_r,$$

wo Δ die Determinante $|\eta_{ij}^r|$ bedeutet, die nicht verschwindet, weil Δ^2 die Discriminante der Form $G(x; a, b)$ ist. Ferner sieht man, daß Δ und Δ_r bei der Vertauschung von $\xi_1, \ldots, \xi_n$

mit $\xi_{i_1}, \ldots, \xi_{i_n}$ sich nur insofern ändern, als gewisse Zeilen vertauscht werden; und zwar ist diese Vertauschung von Zeilen für Δ und Δ_r dieselbe. Es ist also $\Delta\Delta_r$, ebenso wie Δ symmetrisch in den ξ_i und daher eine Größe des ursprünglichen orthoiden Bereichs. Dasselbe gilt demnach für die Größenreihe $\alpha_0, \alpha_1, \ldots$.

Schreibt man nun $F(z)$ als Produkt der beiden Faktoren

$$(z - \xi_i)(z - \xi_j) = z^2 + \sigma_1' z + \sigma_2'$$

und

$$\prod_{(r)}(z - \xi_r) = z^{n-2} + \sigma_1'' z^{n-3} + \cdots + \sigma_{n-2}'',$$

wo r die Reihe der Zahlen 1 bis n mit Ausschluß von i und j durchläuft, so sind zunächst die Koeffizienten $\sigma_1' = -(\xi_i + \xi_j)$, $\sigma_2' = \xi_i \xi_j$, wie unmittelbar ersichtlich, dann aber auch $\sigma_1'', \ldots, \sigma_{n-2}''$ Größen, welche die für σ_{ij} geforderten Eigenschaften besitzen. Für diese ist es nach den Sätzen über reduzierte Formen, insbesondere § 14 des Kap. II klar, daß sie in der Gestalt

$$\sum \gamma_{rs} \xi_i^r \xi_j^s \qquad (r = 0, \ldots, n-1; s = 0, \ldots, n-2)$$

und, da sie sich nicht ändern, wenn ξ_i mit ξ_j vertauscht werden, auch in der Gestalt

$$\frac{1}{2} \sum \gamma_{rs} (\xi_i^r \xi_j^s + \xi_i^s \xi_j^r)$$

geschrieben werden können. Dann ist bei Anwendung der in (σ) gegebenen Bestimmung

$$\sigma_1' = \varphi_1(\eta_{ij}), \quad \sigma_2' = \varphi_2(\eta_{ij}),$$
$$\sigma_k'' = \psi_k(\eta_{ij}) \qquad (k = 0, \cdots, n-2),$$

wo die Koeffizienten der Formen φ und ψ dem ursprünglich vorgelegten Bereiche angehören. Man hat also

$$F(z) = (z^2 + \varphi_1(\eta_{ij}) z + \varphi_2(\eta_{ij})) \times$$
$$\times (z^{n-2} + \psi_1(\eta_{ij}) z^{n-3} + \cdots + \psi_{n-2}(\eta_{ij})),$$

wenn η_{ij} irgend eine der Größen $a(\xi_i + \xi_j) + b\,\xi_i \xi_j$ bedeutet. Es ist demnach

$$F(z) - (z^2 + \varphi_1(x) z + \varphi_2(x))(z^{n-2} + \psi_1(x) z^{n-3} + \cdots + \psi_{n-2}(x))$$

durch jede der Formen $x - a(\xi_i + \xi_j) - b\,\xi_i\xi_j$ und, da diese durchaus im Sinne der Äquivalenz verschiedene lineare Formen sind, auch durch ihr Produkt, das ist $G(x; a, b)$ teilbar. Man ist so zur fundamentalen Gaußschen Identität gelangt:

$$F(z) = (z^2 + \varphi_1(x)z + \varphi_2(x))(z^{n-2} + \psi_1(x)z^{n-3} + \cdots + \psi_{n-2}(x)) + G(x)H(x, z), \qquad (G)$$

wo $G(x)$ vom Grade $\frac{n(n-1)}{2}$ ist und, sowie $H(x, z)$, dem ursprünglichen orthoiden Bereiche angehörige, durch rationale Operationen vollständig bestimmte Koeffizienten besitzt.

§ 28. Der „Fundamentalsatz der Algebra" lautet: Für jede ganze Funktion $F(z)$, deren Koeffizienten beliebige reelle oder komplexe Zahlen sind, und deren Grad $n \geqq 1$ ist, läßt sich eine reelle oder komplexe Zahl ζ bestimmen, so daß $F(\zeta) = 0$ wird.

Der Satz gehört — wie sein Inhalt zeigt — in die Theorie der analytischen Funktionen; der Beweis wird aber bei Benutzung der eben abgeleiteten Identität nicht nur besonders einfach, sondern charakterisiert die bei Auflösung der Gleichung $F(z) = 0$ auftretenden Zahlen auf das genaueste und reduziert endlich das beim Beweise auftretende funktionentheoretische Element auf das Minimum.

Die Gesamtheit der komplexen Zahlen bildet einen orthoiden Bereich; die Identität G ist also anwendbar.

Der Fundamentalsatz gilt ferner jedenfalls für Gleichungen zweiten Grades; in diesem Falle wird die Darstellung der Wurzeln durch gewisse, schon in den Elementen betrachtete Grenzwerte, die s. g. quadratischen Irrationalitäten geliefert.

Die Funktionentheorie gibt ferner durch fundamentale Stetigkeitsbetrachtungen den folgenden speziellen Fall des Fundamentalsatzes: Jede Gleichung mit reellen Koeffizienten, deren Grad eine ungerade Zahl ist, besitzt eine reelle Wurzel.

Für Gleichungen mit reellen Koeffizienten folgt nun die allgemeine Gültigkeit des Fundamentalsatzes durch folgende vollständige Induktion.

Wir setzen voraus, daß der Satz für Gleichungen gilt, deren Gradzahl wohl durch 2^{k-1}, aber nicht durch 2^k teilbar ist, und beweisen, daß er dann auch für solche Gleichungen gilt, deren Grad durch 2^k, aber nicht durch 2^{k+1} teilbar ist.

Sei $F(z) = 0$ eine Gleichung, deren Gradzahl die eben ausgesprochene Eigenschaft besitzt. Dann ist der Grad von $G(x)$, wenn h eine ungerade Zahl ist, $n = 2^k h$, und

$$\frac{n(n-1)}{2} = \frac{2^k h(2^k h - 1)}{2}$$

wohl durch 2^{k-1}, aber nicht durch 2^k teilbar. Die Gleichung $G(x) = 0$ hat also eine Wurzel ξ. Setzt man in der Identität (G) nun $x = \xi$, so wird $G(\xi) = 0$, und

$$F(z) = (z^2 + \varphi_1(\xi) z + \varphi_2(\xi))(z^{n-2} + \psi_1(\xi) z^{n-3} + \cdots + \psi_{n-1}(\xi)),$$

und die Wurzel ζ der Gleichung zweiten Grades

$$z^2 + \varphi_1(\xi) z + \varphi_2(\xi) = 0$$

ergibt auch $F(\xi) = 0$.

Eine ganz elementare Betrachtung erledigt nun auch den Fall komplexer Koeffizienten. Dann kann

$$F(z) = F_1(z) + \sqrt{-1}\, F_2(z)$$

geschrieben werden, wo $F_1(z)$ und $F_2(z)$ reelle Koeffizienten besitzen. Ebenso hat die Gleichung

$$(F_1(z) + \sqrt{-1}\, F_2(z))(F_1(z) - \sqrt{-1}\, F_2(z)) = 0$$

reelle Koeffizienten, sie hat also eine Wurzel $\xi = \alpha + \beta\sqrt{-1}$. Ist nun etwa $F(\alpha + \beta\sqrt{-1})$ von 0 verschieden, so muß

$$F_1(\alpha + \beta\sqrt{-1}) - \sqrt{-1}\, F_2(\alpha + \beta\sqrt{-1}) = 0$$

sein und auch gleich 0 bleiben, wenn man $-\sqrt{-1}$ statt $\sqrt{-1}$ setzt, d. h. es ist dann $F(\alpha - \beta\sqrt{-1}) = 0$. Von den beiden komplexen Zahlen $\alpha \pm \beta\sqrt{-1}$ ist mithin eine jedenfalls Wurzel der Gleichung $F(z) = 0$.

Fünftes Kapitel.

Allgemeine Theorie der Elimination.

Das fundamentale Problem.

§ 1. Mit dem holoiden Bereiche [A] ist der zugeordnete orthoide Bereich (A) und mit diesem das Reich der in Bezug auf (A) algebraischen Größen begrifflich vollständig gegeben. Dieser letztere Bereich, der, wie wir nach den Entwicklungen in Kap. IV wissen, wieder ein orthoider Bereich ist, soll kurz durch das Symbol $\{A\}$ bezeichnet werden. Eine Größe x heiße nun unbeschränkt veränderlich (variabel) in $\{A\}$, wenn für ihre Festsetzung keine weitere Bedingung vorliegt als die, daß sie gleich irgend einer Größe des Bereichs $\{A\}$ sei. Wenn [A] die Gesamtheit der komplexen Zahlen bedeutet, ist die unbeschränkte Veränderlichkeit von x nichts anderes als die freie Variabilität im Sinne der Theorie der analytischen Funktionen.

Wenn im folgenden der zu Grunde liegende Bereich $\{A\}$ ein für allemal festgehalten ist, werden wir, um eine knappere Ausdrucksweise zu gewinnen, bei Bezeichnung einer Größe als unbeschränkt veränderlich den selbstverständlichen Zusatz „in $\{A\}$“ weglassen.

Das Fundamentalproblem der Eliminationstheorie kann sodann folgendermaßen formuliert werden:

Seien $F_j(z_1, z_2, \ldots, z_m)$ $(j = 1, \ldots, k)$ dem orthoiden Bereiche (A) entstammende, nicht identisch verschwindende, aber sonst beliebige Formen; dann bedingt das Gleichungssystem

$$F_j(x_1, x_2, \ldots, x_m) = 0 \qquad (j = 1, 2, \ldots, k)$$

für die ursprünglich als in $\{A\}$ unbeschränkt veränderlich gedachten Größen $x_1, \ldots, x_m$ jedenfalls eine Beschränkung dieser Veränderlichkeit, da ja für $x_1, x_2, \ldots, x_m$ auch schon solche rationale und ganze Zahlen gesetzt werden können, daß der Wert von F_j von 0 verschieden ist. Diese Beschränkung der Veränderlichkeit für $x_1, \ldots, x_m$, die durch ein Gleichungssystem bewirkt wird, vollständig und möglichst einfach zu beschreiben, ist die erste und grundlegende Aufgabe der Eliminationstheorie. Das entsprechende Problem für eine Unbekannte x_1 kann als vollständig gelöst betrachtet werden, da ja in diesem Falle die Veränderlichkeit von x_1 auf eine endliche Anzahl von in Bezug auf (A) algebraischen Größen beschränkt ist, deren vollständige Darstellung in Kap. IV gegeben wurde.

Daß sich nun diese Beschränkung der Veränderlichkeit für Gleichungssysteme ganz anders gestalten kann, ist von vornherein aus dem Umstande klar, daß man in der elementarsten Weise solche Gleichungssysteme bilden kann, denen unendlich viele Wurzelsysteme entsprechen.

Von vornherein soll hier nur jenes prinzipiell wichtigste Resultat unsrer Untersuchung erwähnt werden, daß, wenn das entsprechende Problem für eine Gleichung mit einer Unbekannten als erledigt*) betrachtet wird, die weitere Entwicklung ausschließlich eine bestimmte Reihe „rationaler Operationen" erfordert, worunter die Anwendung der vier Species auf Größen des Bereichs (A) und die Bestimmung des größten gemeinschaftlichen Teilers von dem Bereiche (A) entstammenden Formen verstanden werden soll.

Die Formen F_j enthalten nur eine endliche Reihe von Koeffizienten; selbstverständlich kann demnach für (A) jeder orthoide Bereich genommen werden, der jene als Koeffizienten

*) Dies kann nicht nur in der Auffassung der Theorie der algebraischen Größen geschehen sein, sondern auch so, wie es die Theorie der Funktionen verlangt, wo dann jene Wurzeln der Gleichungen mit einer Unbekannten als Grenzwerte, respektive algebraische Funktionen erscheinen.

auftretenden Größen enthält, so z. B. jeder Bereich (A′), der alle Größen des Bereichs (A) enthält. Dem gegenüber wird der „kleinste“ Bereich, von dem die Untersuchung ausgehen kann, derjenige Rationalitätsbereich sein, der durch die Koeffizienten der Formen F_j vollständig bestimmt ist, und jeder an Stelle von (A) tretende Bereich (A′) wird diesen Rationalitätsbereich „enthalten“.

Der so zu Grunde liegende Bereich (A) kann nun auch Unbestimmte umfassen, die aber dann im Laufe der Untersuchung als solche festzuhalten sind; für diese ist es demnach ihrer begrifflichen Bestimmung nach unstatthaft, von einer Beschränkung der Variabilität zu sprechen. Damit ist die Allgemeinheit der Untersuchung keineswegs beschränkt; es sondern sich nur die verschiedenen Eliminationsprobleme, die demselben Gleichungssysteme $F_j = 0$ entsprechen können, je nachdem wir die verschiedenen x als Unbestimmte oder Unbekannte auffassen*).

Die Kroneckersche Eliminationsmethode.

§ 2. Das aufgestellte Problem wird durch eine von Kronecker**) herrührende, aber nur in knappster Form an-

---

*) So wird z. B. das Gleichungssystem

$$zx + y = 2, \quad x + y = 1,$$

wenn man x und y als Unbekannte, z als Unbestimmte auffaßt, nur die eine Lösung

$$x = \frac{1}{z-1}, \quad y = \frac{z-2}{z-1}$$

zulassen, während, wenn x, y und z gleichmäßig als Unbekannte betrachtet werden, demselben Systeme unendlich viele Lösungen entsprechen, in denen die Veränderlichkeit von x, y und z nun derart beschränkt ist, daß x jeden Wert mit Ausschluß der 0, y jeden Wert mit Ausschluß der 1 und ebenso z jeden Wert mit Ausschluß der 1 annehmen kann und weiter, sobald für eine der Unbekannten irgend ein diesen Bedingungen entsprechender Wert angenommen wird, die beiden andern dadurch vollständig bestimmt sind.

**) Festschrift. § 10. Die dort ausgesprochene Absicht, die Theorie

gedeutete Methode vollständig erledigt. Im wesentlichen ist es schon durch die Aufstellung der Resolventenform des Formensystems F_j und die sich an diese anschließenden Erörterungen (Kap. III. § 18—21) gelöst, und es wird jetzt nur darauf ankommen, die bei der Bildung des größten gemeinschaftlichen Teilers auftretenden Ausnahmefälle (Kap. III. § 20) zu vermeiden und dadurch eine einfache und allgemeine Darstellung zu erhalten. Dies geschieht, wenn wir dem Kroneckerschen Eliminationsprinzip gemäß nicht nur die Formen F_j mit Hilfe neuer Unbestimmten u_j und u_j' in $\sum_{j=1}^{k} F_j u_j$ und $\sum_{j=1}^{k} F_j u_j'$ zusammenfassen, sondern ebenso die Unbestimmten $x_1, \ldots, x_m$ (die ja auch Formen sind) mit Hilfe der Unbestimmten $t_1, \ldots, t_m$ in $\sum_{i=1}^{m} t_i x_i$ vereinigen, ein Verfahren, das sich rechnerisch so ausdrücken läßt, daß wir für x_m durch die lineare Transformation

$$x = t_1 x_1 + t_2 x_2 + \cdots + t_m x_m$$

die neue Unbestimmte x einführen.

Dabei wird es aber zweckmäßig sein, um die Darstellung von unwesentlichen Zufälligkeiten zu befreien, das vorgelegte Formen- resp. Gleichungssystem zuerst einer linearen Transformation zu unterwerfen, deren Koeffizienten sich in jedem einzelnen Falle leicht bestimmen lassen.

Ist nämlich das ursprünglich vorgelegte Gleichungssystem

$$G_j(z_1, z_2, \ldots, z_m) = 0, \qquad (j = 1, \ldots, k)$$

und übt man darauf die lineare Transformation

$$z_i = v_{i1} x_1 + v_{i2} x_2 + \cdots + v_{im} x_m \quad (i = 1, \ldots, m) \qquad \text{(T)}$$

aus, wo die passende Bestimmung der Koeffizienten der Trans-

---

der Elimination in weiteren Abhandlungen ausführlich zu behandeln, ist leider unausgeführt geblieben.

formation vorbehalten bleibt, so erhält man das „transformierte" Gleichungssystem:

$$F_j(x_1, \ldots, x_m) = 0 \qquad (j = 1, \ldots, k),$$

dessen Koeffizienten vorläufig als Formen der v gegeben sind.

Verfährt man nun für dieses System nach der in Kap. III. § 18 gegebenen Anweisung, so werden die dort auftretenden Formen $F_{j_h}^{(h)}, D^{(h)}$ durchweg in Bezug auf $x_{h+1}, \ldots, x_m$ regulär sein, insofern man die in den Koeffizienten auftretenden Größen v als Unbestimmte faßt. Wäre dies für irgend eine dieser Formen, die z. B. mit φ bezeichnet werden soll, zum ersten Male nicht der Fall, also φ eine Form N^{ter} Dimension und nicht regulär, so muß φ jedenfalls eine Form $F_{j_h}^{(h)}$ sein. Sind nämlich für irgend ein h die sämtlichen Formen $F_{j_h}^{(h)}$ regulär, so wird auch ihr größter gemeinschaftlicher Teiler $D^{(h)}$ regulär sein. Ist aber jenes φ eine Form $F_{j_h}^{(h)}$, dann kann man auf die F_j eine solche bestimmte lineare Transformation (T_1) der Unbestimmten $x_{h+1}, \ldots, x_m$ anwenden, daß φ von der Dimension N bleibt, aber regulär wird; während die früheren Formen ihre Dimension behalten und auch regulär bleiben. Die Folge von (T) und (T_1) ergibt daher eine Transformation, bei welcher in φ der Koeffizient von $x_i^N (i = h + 1, \ldots, m)$ immer von 0 verschieden ist, während doch der Annahme nach für jedes Wertsystem der v ein solcher Koeffizient gleich 0 ist. Die Annahme ist demnach unstatthaft, und die aus dem Formensystem F_j gebildeten Formen $F_{j_h}^{(h)}, D^{(h)}$ sind durchweg in Bezug auf $x_{h+1}, \ldots, x_m$ regulär.

Wendet nun auf das Formensystem F_j die weitere lineare Transformation

$$x = t_1 x_1 + t_2 x_2 + \cdots + t_m x_m \qquad (T')$$

an, wo $x_1, \ldots, x_{m-1}$ bleiben und nur x für x_m eingeführt wird, so ist die Folge von T und T' gleichbedeutend mit der Transformation

$$z_i = \left(v_{i1} - v_{im}\frac{t_1}{t_m}\right)x_1 + \left(v_{i2} - v_{im}\frac{t_2}{t_m}\right)x_2 + \cdots + v_{im}\frac{1}{t_m}x \quad (\mathrm{T}'')$$
$$(i = 1, \ldots, m).$$

In dem durch die Transformation (T') aus $F_j = 0$ entstehenden Gleichungssysteme, das mit

$$f_j = 0 \qquad (j = 1, \ldots, k)$$

bezeichnet werden soll, können die Koeffizienten als Formen der t angesehen werden, da man zu diesem Zweck nur mit einer Potenz von t_m zu multiplizieren hat, was im Sinne der Äquivalenzbestimmung gestattet ist*).

Sind nun die bei der Diskussion der Resolventenform des Systems f_j auftretenden Formen

$$D_t^{(h)} \text{ und } f_{j_h}^{(h)},$$

wobei wieder von den als Nenner hinzutretenden Potenzen von t_m als irrelevant abgesehen wird, so werden diese abermals in Bezug auf $x_{h+1}, \ldots, x_{m-1}, x$ regulär sein. Es entsteht nämlich $D_t^{(h)}$ und $f_{j_h}^{(h)}$ aus $D^{(h)}$ und $F_{j_h}^{(h)}$, wenn man an Stelle der v die Koeffizienten der linearen Transformation T'' setzt, die als Folge von T und T' definiert ist, und dann mit einer gewissen Potenz von t_m multipliziert. Die Koeffizienten der für das reguläre Verhalten entscheidenden Glieder sind dann dem Bereiche (A) entstammende Formen der v und t, die nicht identisch verschwinden; denn das ist auch dann nicht der

*) Die zu untersuchenden Formen sind im Sinne der Theorie der Resolventenform als Formen der Unbestimmten x zu betrachten; ihre Koeffizienten gehören jenem orthoiden Bereiche an, der dem Formenbereiche $[(\mathrm{A}), t_1, \ldots, t_m]$ zugeordnet ist, der selbst ein vollständiger holoider Bereich ist. Da nun diese Formen in Bezug auf den Äquivalenzbereich $((\mathrm{A}), t_1, \ldots, t_m)$ zu betrachten sind und äquivalente Formen einander unbedingt ersetzen können, können wir die Nenner immer entfernen und schließlich in den Formen, deren Koeffizienten nun dem vollständigen holoiden Bereiche $[(\mathrm{A}), t_1, \ldots, t_m]$ angehören, den größten gemeinschaftlichen Teiler der Koeffizienten entfernen, d. h. die auftretenden Formen können immer als primitive Formen der Unbestimmten $x_1, \ldots, x_{m-1}$ und x angenommen werden.

Fall, wenn $t_1 = \ldots = t_{m-1} = 0$, $t_m = 1$ gesetzt wird; da man dann wieder die früheren Formen erhält. Man kann daher (auch rationale und ganze) Wertsysteme

$$v_{ij} = a_{ij}$$

bestimmen, für welche diese Koeffizienten nicht verschwindende Formen der t werden, deren Determinante $|a_{ij}|$ von 0 verschieden ist. Damit ist folgendes Resultat gewonnen:

Das ursprüngliche Gleichungssystem $G_j = 0$ geht durch eine bestimmte lineare Transformation (mit nicht verschwindender Determinante) in ein Gleichungssystem $F_j = 0$ von der Beschaffenheit über, daß, wenn dieses durch die weitere Transformation

$$x = t_1 x_1 + \cdots + t_m x_m$$

in das System $f_j = 0$ übergeführt wird, die diesem entsprechenden Formen $D_t^{(h)}, f_h^{(h)}$ durchweg in Bezug auf $x_{h+1}, \ldots, x_{m-1}$ und x regulär sind.

Dabei sind die t als Unbestimmte aufzufassen; doch bleibt der Satz auch dann gültig, wenn statt der t solche Wertsysteme gesetzt werden, bei denen jene im allgemeinen nicht verschwindenden Formen der t von 0 verschiedene Werte annehmen.

§ 3. Die Diskussion der Systeme $G_j = 0$ und $F_j = 0$ bietet völlig identische Probleme, da die ihnen entsprechenden Wertsysteme durch eine lineare Transformation einander in eindeutiger Weise zugeordnet sind. (Die so bestimmte lineare Transformation ist in geometrischer Auffassung nichts anderes als eine einfache Koordinatentransformation.) An Stelle des ursprünglichen Gleichungssystems untersuchen wir also das „von Zufälligkeiten befreite" System $F_j = 0$ und das mit ihm durch die Transformation

$$x = t_1 x_1 + \cdots + t_m x_m$$

zusammenhängende System $f_j = 0$, in welchem, wie schon erwähnt, die Koeffizienten als Formen der Unbestimmten t an-

zusehen sind, was nur die unbedingt gestattete Entfernung des Nenners, einer Potenz von t_m voraussetzt.

Die den Gleichungssystemen $F_j = 0$ und $f_j = 0$ entsprechenden Wertsysteme bedingen sich selbstverständlich gegenseitig. Für die Übersichtlichkeit der weiteren Darstellung wird es bequem sein, dies ausführlich zu formulieren.

Jedes Wertsystem $\xi_1, \xi_2, \ldots, \xi_m$, das dem Gleichungssystem $F_j = 0$ genügt, ergibt ein Wertsystem

$$\xi_1, \xi_2, \ldots, \xi_m, \quad \xi = \sum_{i=1}^{m} t_i \xi_i,$$

das dem Gleichungssysteme

$$F_j = 0, \quad x = t_1 x_1 + \cdots + t_m x_m$$

genügt. Weiter genügt auch, wenn dies der Fall ist,

$$\xi_1, \ldots, \xi_{m-1}, \xi = \sum_{i=1}^{m} t_i \xi_i$$

den Gleichungen $f_j = 0$.

Umgekehrt ergibt jedes Wertsystem

$$\xi_1, \xi_2, \ldots, \xi_{m-1}, \xi,$$

das dem Gleichungssystem

$$f_j = 0 \qquad (j = 1, \ldots, k)$$

genügt, wenn

$$\xi_m = \frac{1}{t_m}(\xi - t_1 \xi_1 - \cdots - t_{m-1} \xi_{m-1})$$

gesetzt wird, ein Wertsystem

$$\xi_1, \ldots, \xi_m, \xi,$$

das den Gleichungen

$$F_j = 0, \quad x = t_1 \xi_1 + \cdots + t_m \xi_m$$

genügt, und, da die Formen F_j die Unbestimmte x überhaupt nicht enthalten, ist endlich auch

$$\xi_1, \xi_2, \ldots, \xi_m, \quad \xi_\tau = \sum_{i=1}^{m} \tau_i \xi_i$$

ein Wertsystem, das dem Gleichungssystem

$$F_j = 0, \quad x = \tau_1 x_1 + \cdots + \tau_m x_m$$

genügt, wo $\tau_1, \ldots, \tau_m$ neue Unbestimmte bedeuten.

§ 4. Es seien nun wieder $D_t^{(h)}$ und $f_{j_h}^h$ die Formen, die bei der Bildung und Diskussion der Resolventenform des Systems f_j auftreten. Dann stellt die Gleichung

$$\Phi_t = D_t D_t^{(1)} \dots D_t^{(m-1)} = 0$$

die Gesamtresolvente des Gleichungssystems $F_j = 0$ dar, in dem Sinne, daß diese Gleichung sämtliche Wurzelsysteme des Systems $F_j = 0$ in vollständiger und einfacher Weise charakterisiert. Der Fußnote zu § 2 dieses Kap. entsprechend sind dabei $D_t, D_t^{(1)}, \dots$ und also auch Φ_t primitive Formen von $x, x_1, \dots, x_{m-1}$, deren Koeffizienten dem Formenbereiche $[(\mathsf{A}), t_1, \dots, t_m]$ angehören. Dabei ist $D_t^{(h)}$ oder, ausführlich geschrieben,

$$D_t^{(h)} = D_t^{(h)}(x;\ x_{h+1}, \dots, x_{m-1};\ t_1, \dots, t_m)$$

eine reguläre Form der Unbestimmten $x, x_{h+1}, \dots, x_{m-1}$, kann aber auch von der Dimension 0 sein und ist dann unsern Festsetzungen gemäß gleich Eins zu setzen.

Ist $\Phi_t = \Psi_t X_t$, so soll $\Psi_t = 0$ eine Teilresolvente des Gleichungssystems $F_j = 0$ heißen; insbesondere sollen die Gleichungen $D_t^{(h)} = 0$ als vollständige (Teil-)Resolventen $h + 1^{\text{ter}}$ Stufe des Systems $F_j = 0$ bezeichnet werden. Eine solche Resolvente „existiert nicht", wenn $D_t^{(h)}$ gleich Eins ist.

Irgend eine der Kongruenzen $(\overline{R})$ in Kap. III. § 18 lautet jetzt

$$D_t D_t^{(1)} \dots D_t^{(m-1)} C \equiv 0 \,(\text{mod. } f_1, \dots, f_k), \qquad (C)$$

wo C dem Formenbereiche $[(\mathsf{A}), t_1, \dots, t_m]$ angehört und von 0 verschieden ist. Da ferner für $x = t_1 x_1 + \dots + t_m x_m$ der Definition nach $f_j = t_m^{a_j} F_j$ ist, wird $f_j - t_m^{a_j} F_j$ als Form der x durch $x - t_1 x_1 - \dots - t_m x_m$ teilbar, und die Kongruenz (C) erhält die neue Gestalt:

$$D_t D_t^{(1)} \dots D_t^{(m-1)} C \equiv 0 \left(\text{mod. } F_1, \dots, F_k, x - \sum_{i=1}^{m} t_i x_i\right).$$

Ist $x_1 = \xi_1, \dots, x_m = \xi_m$ irgend ein Wurzelsystem des Systems $F_j = 0$ und $x = \xi = \sum_{i=1}^{m} t_i \xi_i$, so muß einer der

Faktoren $D_t^{(h)}$ verschwinden; denn C ist eine von den x unabhängige, von 0 verschiedene Größe.

Wenn umgekehrt $x_{h+1} = \xi_{h+1}, \ldots, x_{m-1} = \xi_{m-1}, x = \xi$ ein solches Wertsystem darstellt, für welches $D_t^{(h)}$ Null wird, so gibt es nach den wiederholt angeführten Erörterungen des Kap. III (insbesondere § 20) eine endliche Anzahl von Wertsystemen für $x_1, \ldots, x_h$, zumindest eines von der Beschaffenheit, daß jedes f_j gleich Null wird, und

$$\xi_1, \xi_2, \ldots, \xi_{m-1}, \xi_m = \frac{1}{t_m}(\xi - t_1\xi_1 - \cdots - t_{m-1}\xi_{m-1})$$

ist nach dem Vorhergehenden ein Wurzelsystem der Gleichungen $F_j = 0$.

Wir haben nun den folgenden für die Theorie der Elimination grundlegenden Satz nachzuweisen:

Setzt man in $D_t^{(h)}(x; x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m)$ für die Unbestimmten $x_{h+1}, \ldots, x_{m-1}$ irgend welche Größen $\xi_{h+1}, \ldots, \xi_{m-1}$, so wird

$$D_t^{(h)}(x; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)$$

eine homogene Form von $x, t_1, \ldots, t_m$ und ist, wenn $D_t^{(h)}$ von 1 verschieden ist, als solche in der Gestalt eines Produktes linearer Formen derselben Unbestimmten darstellbar.

Die Koeffizienten von $D_t^{(h)}(x; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)$ sind aus Größen des Bereichs (A) und $\xi_{h+1}, \ldots, \xi_{m-1}$ durch Addition und Multiplikation zusammengesetzt, bestimmen also einen bestimmten Rationalitätsbereich (R), und es ist endlich ein diesem entstammender Gattungsbereich, in dem jene Zerlegung stattfindet.

Zum Beweise des Satzes führen wir die weiteren beliebig gewählten Größen $\xi_1, \ldots, \xi_h$ ein und bezeichnen das Resultat der Substitution von $\xi_1, \ldots, \xi_{m-1}$ für $x_1, \ldots, x_{m-1}$ in $D_t^{(h)}$ und Φ_t mit $\overline{D}_t^{(h)}$ und $\overline{\Phi}_t$. Diese letzteren Formen (von $x, t_1, \ldots, t_m$) können mehrfache Teiler besitzen; um sie zu entfernen, bilden wir den größten gemeinschaftlichen Teiler von $\overline{D}_t^{(h)}$ und $\frac{\partial}{\partial x}\overline{D}_t^{(h)}$, resp. $\overline{\Phi}_t$ und $\frac{\partial}{\partial x}\overline{\Phi}_t$ und entfernen ihn

aus $\overline{D}_t^{(h)}$ und $\overline{\Phi}_t$. Dann seien $\overline{E}_t^{(h)}$, bez. $\overline{\Psi}_t$ das Produkt der einfachen Teiler von $\overline{D}_t^{(h)}$, bez. $\overline{\Phi}_t$. Jedenfalls ist dann

$$\overline{\Psi}_t = \overline{E}_t^{(h)} \overline{X}_t^{(h)}.$$

Aus der Gleichung

$$\overline{E}_{t'}^{(h)} = 0,$$

wo $t'_1, \ldots, t'_m$ eine neue Reihe von Unbestimmten bedeutet, die mit $t_1, \ldots, t_m$ gleichberechtigt ist, erhält man in einem bestimmten, dem Bereiche $((A), t'_1, \ldots, t'_m)$ entstammenden Gattungsbereiche für x als Unbekannte gewisse diesem Gattungsbereiche angehörige Größen als Wurzeln der Gleichung. Sei eine derselben ξ'. Für diese ist jedenfalls auch $\overline{D}_{t'}^{(h)} = 0$, und man erhält demnach durch den in Kap. III. § 20 erläuterten Algorithmus wenigstens ein Größensystem

$$\xi', \xi'_1, \ldots, \xi'_h$$

von der Beschaffenheit, daß

$$\xi', \xi'_1, \ldots, \xi'_h, \xi_{h+1}, \ldots, \xi_{m-1}$$

dem Gleichungssystem $[f_j]_{t'} = 0$ genügt*). Fügt man diesen Größen die durch die Gleichung

$$\xi' = \sum_{r=1}^{h} \xi'_r t'_r + \sum_{s=h+1}^{m-1} \xi_s t'_s + \xi'_m t'_m \qquad (\xi')$$

definierte Größe ξ'_m hinzu, so genügt das Wertsystem

$$\xi', \xi'_1, \ldots, \xi'_h, \xi_{h+1}, \ldots, \xi_{m-1}, \xi'_m$$

auch den Gleichungen

$$[f_j]_{t'} = 0, \quad x = t'_1 x_1 + \cdots + t'_m x_m$$

und also auch dem Systeme

$$F_j = 0, \quad x = t'_1 x_1 + \cdots + t'_m x_m.$$

Da die Formen F_j die Unbestimmte x gar nicht enthalten, genügt endlich das Größensystem

und $$\xi'_1, \ldots, \xi'_h, \xi_{h+1}, \ldots, \xi_{m-1}, \xi'_m$$

*) Wo $[f_j]_{t'}$ jene Form bedeutet, die aus f_j entsteht, wenn man $t'_1, \ldots, t'_m$ an Stelle von $t_1, \ldots, t_m$ setzt.

$$\xi_t = \sum_{r=1}^{h} \xi'_r t_r + \sum_{s=h+1}^{m-1} \xi_s t_s + \xi'_m t_m ,$$

wo $t_1, \ldots, t_m$ die zuerst benutzten Unbestimmten sind, auch dem Systeme

$$F_j = 0 , \quad x = t_1 x_1 + \cdots + t_m x_m$$

oder endlich den Gleichungen $f_j = 0$.

Für diese Größen wird also $\overline{\Phi}_t$ und auch $\overline{\Psi}_t$ gleich Null; demnach endlich auch $\overline{E}_t^{(h)}$ oder $\overline{X}_t^{(h)}$. Dabei unterscheiden sich $\overline{\Phi}_t$ u. s. w. von den Größen $\overline{\Phi}_{t'}$ u. s. w. nur in der Bezeichnung der Unbestimmten t.

Betrachtet man aber in der Gleichung

$$\overline{X}_t^{(h)} = 0$$

x als Unbekannte, so kann diese die Wurzel

$$\xi_t = \sum_{r=1}^{h} \xi'_r t_r + \sum_{s=h+1}^{m-1} \xi_s t_s + \xi'_m t_m$$

nicht besitzen; sonst hätte, da die t eben Unbestimmte sind, die Gleichung $\overline{X}_t^{(h)} = 0$ die entsprechende Wurzel

$$\xi' = \sum_{r=1}^{h} \xi'_r t'_r + \sum_{s=h=1}^{m-1} \xi_s t'_s + \xi'_m t'_m ,$$

die der für ξ'_m gegebenen Definition gemäß auch der Gleichung $\overline{E}_{t'}^{(h)} = 0$ genügt; während doch ihrer Bildung entsprechend $\overline{E}_{t'}^{(h)}$ und $\overline{X}_{t'}^{(h)}$ keinen gemeinschaftlichen Teiler besitzen.

Es hat demnach $\overline{E}_t^{(h)}$ und auch $\overline{D}_t^{(h)}$ den linearen Teiler

$$L_1 = x - \sum_{r-1}^{h} \xi'_r t_r - \sum_{s=h+1}^{m-1} \xi_s t_s - \xi'_m t_m .$$

Entfernt man den so bestimmten linearen Teiler aus $\overline{E}_t^{(h)}$ und schlägt ihn zu $\overline{X}_t^{(h)}$, so läßt sich die eben ausgeführte Schlußweise genau wiederholen, und man erhält, dem angekündigten Satze entsprechend,

$$\overline{E}_t^{(h)} = T_h^{\nu_h} L_1 \ldots L_{\nu_h}$$

$$L_k = x - \sum_{r=1}^{h} \xi_r^{(k)} t_r - \sum_{s=h+1}^{m-1} \xi_s t_s - \xi_m^{(k)} t_m \qquad (k = 1, \ldots \nu_h),$$

wenn ν_h den Grad von $\overline{E}_t^{(h)}$ in x bezeichnet, und

$$\overline{D}_t^{(h)} = T_h L_1^{c_{h1}} \dots L_{\nu_h}^{c_{h\nu_h}},$$

wo die $c_{h\nu_h}$ positive ganze Zahlen bedeuten.

Dabei ist aber noch nachzuweisen, daß T_h eine Größe des Bereichs (A) ist und also gleich Eins gesetzt werden kann. Es ist T_h nichts anderes als der Koeffizient der höchsten Potenz von x in $\overline{D}_t^{(h)}$. Da aber $D_t^{(h)}$ eine reguläre Form der x ist, so enthält dieser Koeffizient keine der Unbestimmten $x_{h+1}, \dots, x_{m-1}$, und bleibt demnach bei Einsetzung irgend eines Größensystems $\xi_{h+1}, \dots, \xi_{m-1}$ dieselbe, dem Bereiche (A) entstammende Form der Unbestimmten t.

Man kann aber auch $\xi_{h+1}, \dots, \xi_{m-1}$ geradezu als Unbestimmte wählen, d. h. $x_{h+1}, \dots, x_{m-1}$ als solche belassen. Dann beziehen sich unsre Schlüsse auf $D_t^{(h)}$ selbst. Wäre nun T_h eine wirkliche Form der t, so hätte man $D_t^{(h)}$ im Widerspruche mit unsern Festsetzungen durch T_h teilbar und nicht als primitive Form gefaßt; es ist also T_h in der Tat eine Größe des Bereichs (A) und ~ 1. Wenn man daher $D_t^{(h)}$ durch T_h dividiert und diese Gestalt der Form zu Grunde legt, kann schließlich auch $T_h = 1$ angenommen werden.

Endlich zeigt noch eine leichte Überlegung, daß die in den Linearfaktoren auftretenden Koeffizienten $\xi_1^{(k)}, \dots, \xi_h^{(k)}, \xi_m^{(k)}$ schon in Bezug auf (R) algebraische Größen sind, d. h. die Unbestimmten t' bei ihrer Bestimmung nur scheinbar auftreten.

Um dies genau auszuführen, denke man sich die Zerlegung von $\overline{D}_t^{(h)}$ auch in der Weise ausgeführt, daß man statt der Unbestimmten $t'_1, \dots, t'_m$ eine dritte Reihe gleichberechtigter Unbestimmter einführt, die mit $t''_1, \dots, t''_m$ bezeichnet werden mag. Dabei erhält man — genau wie früher — eine Zerlegung von $\overline{D}_t^{(h)}$ in Linearfaktoren

$$\overline{D}_t^{(h)} = A_1^{a_{h1}} A_2^{a_{h2}} \dots A_{\nu_h}^{a_{h\nu_h}},$$

wo schon, wie früher, $T = 1$ angenommen ist, und es ist

$$\Delta_k = x - \sum_{r=1}^{h} \eta_r^{(k)} t_r - \sum_{s=h+1}^{m-1} \xi_s t_s - \eta_m^{(k)} t_m,$$

wo $\xi_i^{(k)}$ und $\eta_i^{(k)}$ sich nur dadurch unterscheiden, daß bei der Definition der einen die Unbestimmten t', bei der andern die Unbestimmten t'' benutzt werden.

In dem Gattungsbereiche, der die Größen

$$\xi_i^{(j)},\ \eta_i^{(j)} \qquad (i = 1, \ldots, h, m;\ j = 1, \ldots, \nu_h)$$

sämtlich enthält, ist nun eine zweifache Zerlegung von $\bar{D}_t^{(h)}$ in lineare, also auch irreduzible Faktoren gegeben; es muß also je ein Δ_j je einem L_k äquivalent sein, und es ist schließlich, da der Koeffizient von x in beiden die Einheit ist, auch $L_k = \Delta_j$; d. h.

$$\xi_r^{(k)} = \eta_r^{(j)}. \qquad (r = 1, \ldots, h, m)$$

Nun genügt $\xi_r^{(k)}$ einer Gleichung, deren Koeffizienten dem Bereiche (R) entstammende Formen von $t_1', \ldots, t_m'$ sind, und ebenso $\eta_r^{(j)}$ einer Gleichung, deren Koeffizienten dem Bereiche (R) entstammende Formen von $t_1'', \ldots, t_m''$ sind. Seien diese Gleichungen $\varphi_1 = 0$ und $\varphi_2 = 0$, so haben φ_1 und φ_2 wegen $\xi_r^{(k)} = \eta_r^{(j)}$ einen gemeinsamen Teiler φ und $\xi_r^{(k)} = \eta_r^{(j)}$ genügt schon der Gleichung $\varphi = 0$. Es kann aber φ weder ein t' noch ein t'' enthalten; im ersten Falle könnte φ_2, im zweiten φ_1 nicht durch φ teilbar sein.

Die Größe $\xi_r^{(k)}$ genügt also einer Gleichung, deren Koeffizienten dem Bereiche (R) angehören, und dies sollte eben erwiesen werden.

Selbstverständlich ist dann $j = k$, $a_{h1} = c_{h1}$ u. s. w.

Die Gesamtheit der Lösungen des Systems $F_j = 0$.

§ 5. Die vorstehenden Entwicklungen bieten alle Hilfsmittel, um die durch das Gleichungssystem

$$F_j = 0 \qquad (j = 1, \ldots, k)$$

bewirkte Beschränkung der Veränderlichkeit für die Unbekannten $x_1, \ldots, x_m$ vollständig zu beschreiben. Dabei kann

und soll das Gleichungssystem durch eine passend gewählte lineare Transformation schon in dem früher normierten Sinne von „Zufälligkeiten" befreit sein. Die Koeffizienten des Gleichungssystems mögen dem orthoiden Bereiche (A) angehören, und die Veränderlichkeit der Unbekannten in {A} untersucht werden; diese Festsetzungen fixieren nur die Grundlagen der Untersuchung, ohne deren Allgemeinheit zu beschränken.

Die Gesamtheit der Wurzelsysteme

$$x_1 = \xi_1, \ldots, x_m = \xi_m,$$

die den Gleichungen $F_j = 0$ genügen, soll kurz als der Inhalt des Gleichungssystems bezeichnet werden.

Man erhält demnach den Inhalt des Systems $F_j = 0$, wenn man der Reihe nach die von 1 verschiedenen Formen $D_t^{(h)}$ nimmt, in jeder für $x_{h+1}, \ldots, x_{m-1}$ die beliebigen Größen $\xi_{h+1}, \ldots, \xi_{m-1}$ setzt und dann nach Kap. III. § 20 die Systeme von Größen $\xi_1, \ldots, \xi_h, \xi$, sowie die weitere Größe ξ_m auf Grund von

$$\xi = \sum_{i=1}^{m} \xi_i t_i = \xi_t$$

bestimmt. Dabei ist, ebenso wie $\xi_1, \ldots, \xi_h$, auch ξ_m von den t unabhängig. Es ist dann

$$D_t^{(h)}(\xi_t, \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m) = 0$$

oder also $x - \xi_t = x - \sum_{i=1}^{m} \xi_i t_i$ ein linearer Teiler von $\overline{D}_t^{(h)}$.

Man kann dieses Resultat auch folgendermaßen aussprechen:

Jedes aus der Resolvente $h+1^{\text{ter}}$ Stufe $D_t^{(h)} = 0$ hergeleitete Wurzelsystem $\xi_1, \ldots, \xi_m$ genügt der Gleichung

$$D_t^{(h)}(x_1 t_1 + \cdots + x_m t_m; x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m) = 0,$$

in welcher $t_1, \ldots, t_m$ als Unbestimmte, die Unbekannten $x_1, \ldots, x_m$ als in {A} veränderliche Größen zu fassen sind.

Auch die Umkehrung dieses Satzes ist richtig:

Ist $x_1 = \xi_1, \ldots, x_m = \xi_m$ eine Lösung der eben hingeschriebenen Gleichung in dem angegebenen Sinne, so entsteht diese Lösung in der bekannten Weise aus $D_t^{(h)} = 0$, indem man hierin $x_{h+1} = \xi_{h+1}, \ldots, x_{m-1} = \xi_{m-1}$ setzt und die weiteren Größen $\xi_1, \ldots, \xi_h, \xi_m$ durch die zugehörige Gleichungskette bestimmt.

Denn aus jeder solchen Größenreihe erhält man ein $\xi = \sum_{i=1}^{m} \xi_i t_i$, das nach den soeben abgeschlossenen ausführlichen Entwicklungen der Relation

$$D_t^{(h)}(\xi;\ \xi_{h+1}, \ldots, \xi_{m-1};\ t_1, \ldots, t_m) = 0$$

identisch genügt.

Selbstverständlich gelten die beiden Sätze auch für jeden Teiler von $D_t^{(h)}$, insbesondere also für die einfacheren Formen $E_t^{(h)}$, die aus $D_t^{(h)}$ durch Entfernung des größten gemeinschaftlichen Teilers von $D_t^{(h)}$ und $\frac{\partial}{\partial x} D_t^{(h)}$ entsteht. Man erhält die der Resolvente $h+1^{\text{ter}}$ Stufe entsprechenden Lösungen schon aus der Gleichung

$$E_t^{(h)}\left(\sum_{i=1}^{m} x_i t_i;\ x_{h+1}, \ldots, x_{m-1};\ t_1, \ldots, t_m\right) = 0,$$

die als reduzierte vollständige Resolvente $h+1^{\text{ter}}$ Stufe bezeichnet werden soll, wo jeder Faktor von $D_t^{(h)}$ nur einfach auftritt. Allerdings entgeht dabei eine charakteristische Eigenschaft der Lösung, deren „Multiplizität", der weiteren Untersuchung*); der Inhalt der Gleichungen $F_j = 0$ wird aber schon durch die Gleichungen $E_t^{(h)} = 0$ vollständig beschrieben.

---

*) Die hier zuerst gegebene allgemeinere Fassung der Kroneckerschen Eliminationsmethode geht insofern über die Darstellung der „Festschrift" hinaus, als sie die s. g. Multiplizität der Lösungen nicht vernachlässigt. Die Methode trennt bloß — und zwar in vollständig naturgemäßer Weise — die beiden Probleme, nach denen zuerst die Lösungen von $F_j = 0$ zu bestimmen sind, und dann eine diesen Lösungen zukommende Wertigkeit, die Multiplizität, festgesetzt wird. Die kurze Anzeige der Methode, wie sie die Festschrift

Es muß noch ausdrücklich hervorgehoben werden, daß wegen der Bedeutung der x und t die Gleichung

$$E_t^{(h)}\left(\sum_{i=1}^{m} x_i t_i;\ x_{h+1}, \ldots, x_{m-1};\ t_1, \ldots, t_m\right) = 0$$

und ebenso die entsprechende $D_t^{(h)} = 0$ in Wirklichkeit ein System von Gleichungen in formaler Zusammenfassung darstellt, denn es muß, wenn nach den Potenzprodukten der t geordnet wird, jeder Koeffizient (eine ganze Funktion der x) für sich gleich Null sein.

Das der Gleichung $E_t^{(h)} = 0$ entsprechende Gleichungssystem soll kurz durch E_h bezeichnet werden.

§ 6. Damit ist eine charakteristische Zerlegung des Inhalts der Gleichungen $F_j = 0$ gewonnen. Der Inhalt jedes Systems E_h ist darin enthalten, und der Inhalt der verschiedenen Systeme E_h erschöpft den Inhalt des Systems $F_j = 0$ vollständig.

Der Inhalt des Systems E_h ist „eine dem Bereiche $\{\mathsf{A}\}$ entstammende $(m-h-1)$-fache Mannigfaltigkeit", denn man erhält jedes ihrer „Elemente" und nur solche, wenn

---

bietet, kennt nur die hier von uns als „reduzierte" Resolventen eingeführten Gleichungen $E_t^{(h)} = 0$.

Daneben haben aber die den linearen Faktoren $D_t^{(h)}$ zukommenden Exponenten gleichfalls ihre Bedeutung für das Gleichungssystem und geben geradezu die Grundlage für eine Theorie der Multiplizität der Lösungen in Gleichungssystemen von der hier betrachteten Allgemeinheit. Diese Fragestellung ist bisher nicht weiter verfolgt worden.

Die Theorie der Multiplizität im gewöhnlichen, viel engeren Sinne des Wortes findet sich in Kap. VI, § 27 u. 28.

Die hier gegebene Verallgemeinerung der Kroneckerschen Eliminationstheorie wird insbesondere dadurch wichtig, daß Φ_t, die Resolventenform des Systems f_j, immer $\equiv 0$, (mod. $F_1, \ldots, F_k$) ist. Unter anderem wird hierdurch die vollständige Lösung der in Kap. VII und VIII behandelten arithmetischen Probleme ermöglicht.

Mit der ursprünglichen Kroneckerschen Theorie haben sich noch Molk in der schon früher citierten Abhandlung (Acta math. Bd. VI) und Netto („Vorlesungen über Algebra" II. Bd., pag. 127) beschäftigt.

man in dem Wertsystem $(\xi_1, \ldots, \xi_m)$ die Größen $\xi_{h+1}, \ldots, \xi_{m-1}$, der Anzahl nach $m - h - 1$, beliebig wählt und für die übrigen $\xi_1, \ldots, \xi_h, \xi_m$ die in endlicher Anzahl vorhandenen Wertsysteme einsetzt. Die Anzahl dieser Wertsysteme ist im allgemeinen — mit dem Grade von $E_t^{(h)}$ in x — gleich μ_h, und die so erhaltene Mannigfaltigkeit soll dementsprechend als vom μ_h^{ten} Grade bezeichnet werden.

Dabei bedeutet $E_t^{(h)}$ das Produkt der einfachen Faktoren von $D_t^{(h)}$, insofern $x_{h+1}, \ldots, x_{m-1}$ als Unbestimmte gelten. In dieser Auffassung ist die Discriminante von $E_t^{(h)}$ nach x eine von 0 verschiedene Form von $x_{h+1}, \ldots, x_{m-1}$, und, solange $\xi_{h+1}, \ldots, \xi_{m-1}$ ein solches Größensystem ist, bei dessen Einsetzung diese Discriminante nicht verschwindet, haben $E_t^{(h)}$ und $\bar{E}_t^{(h)}$ in x denselben Grad. Verschwindet aber diese Discriminante für ein gewisses Größensystem $\xi_{h+1}, \ldots, \xi_{m-1}$, so wird $E_t^{(h)}(x; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)$ mehrfache Linearfaktoren enthalten; dabei ist μ_h größer als ν_h, der Grad von $\bar{E}_t^{(h)} = 0$, und daher die Anzahl der einem solchen Systeme entsprechenden Wertsysteme $\nu_h < \mu_h$.

Um dem Satze von der Anzahl der Wertsysteme seine volle Allgemeinheit zu erhalten, zählen wir das zugehörige System der Werte $\xi_1', \ldots, \xi_h', \xi_m'$ so oft, als es der Exponent des entsprechenden Linearfaktors von

$$E_t^{(h)}(x; \xi_{h+1}, \ldots, \xi_{m-1}; t_1, \ldots, t_m)$$

angibt, und nennen das so bestimmte Element der Mannigfaltigkeit ein mehrfaches (Doppel-)Element oder auch singuläres Element; man pflegt sich auch so auszudrücken, daß in diesem singulären Elemente mehrere einfache Elemente „zusammenfallen“*).

Bezeichnet man die Discriminante von $E_t^{(h)}$ nach x mit $\Delta_t^{(h)}$, so definiert die Gleichung

---

*) Um Mißverständnisse zu vermeiden, sei nochmals betont, daß wir bei diesen Begriffsbestimmungen von der durch $E_t^{(h)} = 0$ definierten Mannigfaltigkeit ausgehen, wo $E_t^{(h)}$ als Form der Unbestimmten $x, x_{h+1}, \ldots, x_{m-1}$ keine mehrfachen Faktoren besitzt.

$$\Delta_t^{(h)}(x_{h+1}, \ldots, x_{m-1}; t_1, \ldots, t_m) = 0,$$

die wieder als formale Zusammenfassung eines Gleichungssystems aufzufassen ist, diejenigen Wertsysteme $\xi_{h+1}, \ldots, \xi_{m-1}$, welche singuläre Elemente ergeben, und es ist unmittelbar klar, daß das in den Gleichungen

$$E_t^{(h)} = 0, \quad \frac{\partial}{\partial x} E_t^{(h)} = 0,$$

formal zusammengefaßte Gleichungssystem die singulären Elemente der durch $E_t^{(h)} = 0$ definierten Mannigfaltigkeit und nur diese definiert.

In naturgemäßer Weise erweitern wir den Begriff der aus {A} entstammenden algebraischen Mannigfaltigkeit, indem wir darunter die Gesamtheit aller Wertsysteme $\xi_1, \ldots, \xi_m$ verstehn, die den Gleichungen $F_j = 0$ genügen. Dabei werden wir die genauere Bezeichnung der Mannigfaltigkeit als „algebraische" nicht weiter hinzufügen, da den Zielen der hier dargelegten Theorie gemäß in diesem Buche überhaupt keine anderen betrachtet werden. Auch die zu Grunde liegende m-fache Mannigfaltigkeit $(x_1, \ldots. x_m)$, wo jedes x gleich jeder Größe aus {A} gesetzt werden kann, ist in dem Sinne eine algebraische, da sie durch die Gleichung $0 = 0$ definiert wird, die für die Veränderlichen x keine Beschränkung ergibt.

Im Gegensatze hierzu wird z. B. die Bedingung, daß die x rationale und ganze Zahlen seien, keine algebraische, sondern eine transcendente Mannigfaltigkeit definieren*).

---

*) Diese Begriffsbestimmungen behalten ihre Gültigkeit auch dann, wenn das vorgelegte Gleichungssystem

$$G_j(z_1, \ldots, z_m) = 0$$

ohne vorhergehende lineare Transformation der Untersuchung zu Grunde gelegt wird. Die dabei auftretenden Ausnahmefälle entstehen dadurch, daß die zur Bildung der Gleichungen benutzten Formen nicht mehr regulär sind. Wenn aus den Werten von $z_{h+1}, \ldots, z_{m-1}$ weiter $z_h, \ldots$ bestimmt werden soll, kann der Koeffizient der höchsten Potenz $z_h, \ldots$ verschwinden und die Anzahl der entsprechenden Wert-

Sind demnach für das Gleichungssystem $G_j = 0$ die Formen

$$D_t^{(h_1)}, \quad D_t^{(h_2)}, \ldots$$

im Sinne der Äquivalenz von 1 verschieden, so besteht der Inhalt des Gleichungssystems aus einer $(m - h_1 - 1)$-fachen, einer $(m - h_2 - 1)$-fachen Mannigfaltigkeit u. s. f. Es kann daher — in geometrischer Ausdrucksweise — durch das Gleichungssystem $G_j = 0$ „im Raume von m Dimensionen" eine Anzahl von Gebilden verschiedener Ausdehnung, „Punkte", „Linien", „Flächen", dreifach ausgedehnte Gebilde u. s. f. simultan definiert werden.

Im Interesse einer einheitlichen Nomenklatur machen wir noch die folgende Festsetzung: Die durch das Gleichungssystem $F_j = 0$ definierte Mannigfaltigkeit sei von der $h + 1^{\text{ten}}$ Stufe (vom $h + 1^{\text{ten}}$ Range), wenn h die kleinste ganze Zahl ist, für welche $D_t^{(h)}$ im Sinne der Äquivalenz von Eins verschieden ist (für D_t ist $h = 0$ anzunehmen); dieselbe Be-

---

systeme unter μ_h herabsinken, auch dann, wenn die mehrfachen Elemente mehrfach gezählt werden. Um auch in diesen Fällen die Zahl μ_h wenigstens formell konstant zu erhalten, werden die s. g. „unendlichen" Elemente der Mannigfaltigkeit eingeführt. Es kann weiter auch durch Verschwinden sämtlicher Koeffizienten die Gleichung für $z_h, \ldots$ eine identische werden, ein Fall, der durch das Beispiel einer Fläche, welche die Gerade $x = a$, $y = b$ vollständig enthält, einfach illustriert wird. Alle diese Ausnahmefälle können aber nur dann auftreten, wenn $z_{h+1}, \ldots, z_{m-1}$ einer algebraischen Gleichung $\varphi(z_{h+1}, \ldots, z_{m-1}) = 0$ genügen.

Solche Zufälligkeiten werden durch die gegenseitig eindeutige Beziehung der Mannigfaltigkeiten $(z_1, \ldots, z_m)$ und $(x_1, \ldots, x_m)$ vermieden, die durch die lineare Transformation

$$z_i = \sum_{j=1}^{m} a_{ij} x_j, \quad |a_{ij}| \neq 0$$

gegeben ist. In geometrischer Auffassung hat man sich dabei jedes Element der ersten Mannigfaltigkeit durch die „Koordinaten" $x_1, \ldots, x_m$ gegeben zu denken, was sich unmittelbar auf die in darin enthaltenen $(m-1)$-, $(m-2)$-, ...-fachen Mannigfaltigkeiten überträgt.

nennung wird auch auf das Gleichungssystem $F_j = 0$ und auf das orthoide Formensystem*) F_j übertragen.

Das System $h + 1^{\text{ter}}$ Stufe $F_j = 0$ und die zugehörige Mannigfaltigkeit $h + 1^{\text{ter}}$ Stufe heiße ein reines System, resp. eine reine Mannigfaltigkeit $h + 1^{\text{ter}}$ Stufe, wenn, sobald $k > h$ ist, $D_t^{(k)} \sim 1$ wird. Im entgegengesetzten Falle haben wir ein gemischtes System, resp. eine gemischte Mannigfaltigkeit $h + 1^{\text{ter}}$ Stufe.

Es wird angezeigt sein, in diesem Sinne auch von Systemen $m + 1^{\text{ter}}$ Stufe zu sprechen, die dann „keinen Inhalt" besitzen. Dem Gleichungssysteme $F_j = 0$ entspricht eben in diesem Falle gar kein Wurzelsystem.

Selbstverständlich ist, sobald $D_t^{(h)}$ nicht ~ 1, das in

$$D_t^{(h)} = 0 \quad \text{oder} \quad E_t^{(h)} = 0$$

zusammengefaßte Gleichungssystem von der $h + 1^{\text{ten}}$ Stufe, was mit der früheren Benennung dieser Resolvente übereinstimmt.

Als kurzes Zeichen für eine Mannigfaltigkeit (Varietät) $h + 1^{\text{ter}}$ Stufe benutzen wir $V^{(h+1)}$.

Die singulären Elemente der durch $D_t^{(h)} = 0$ bestimmten $V^{(h+1)}$ ergeben, wie die sie definierenden Gleichungen unmittelbar zeigen, eine Mannigfaltigkeit, deren Stufenzahl zumindest $h + 2$ ist. Sie kann aber auch größer sein und selbst bis zu $m + 1$ steigen, d. h. es gibt Mannigfaltigkeiten, die überhaupt kein singuläres Element besitzen. Nächst dem trivialen Beispiele der durch eine lineare Gleichung definierten $V^{(1)}$ weiß man aus den Elementen der analytischen Geometrie,

---

*) Insofern die Koeffizienten der Formen einem echten holoiden Bereiche angehören und die Problemstellung die Beschränkung auf diesen Bereich fordert, insofern es sich also um im engeren Sinne des Wortes arithmetische Fragen handelt, wird die Stufenzahl des Formensystems F_j nicht mehr mit der des Gleichungssystems $F_j = 0$ übereinstimmend definiert werden können. Sobald wir von einem „Gleichungssystem" sprechen, hat man eben den holoiden Bereich, dem die Formen F_j entstammen, zu dem zugeordneten orthoiden Bereiche erweitert.

daß die „allgemeine" Gleichung zweiten Grades (nicht zerfallender Kegelschnitt u. s. w.) eine solche Mannigfaltigkeit definiert.

§ 7. Wir kehren zur Gesamtresolvente des Gleichungssystems $F_j = 0$ zurück. Diese ist

$$\Phi_t = D_t D_t^{(1)} \dots D_t^{(m-1)} = 0 .$$

Die links stehende Resolventenform ist eine Form der Unbestimmten x; $x_1, \dots, x_{m-1}$; $t_1, \dots, t_m$ mit dem orthoiden Bereiche (A) angehörenden Koeffizienten.

Man sieht zuerst unmittelbar, daß die so interpretierten Formen $D_t^{(h)}$ und $D_t^{(k)}$ $(h \neq k)$ keinen gemeinschaftlichen Teiler besitzen. Dies ergibt sich rein formal aus dem Umstande, daß $D_t^{(h)}$ und $D_t^{(k)}$ als Formen der in ihnen wirklich auftretenden x regulär und primitiv sind.

Die Zerlegung von $D_t^{(h)}$ in irreduzible Faktoren ergibt daher:

$$D_t^{(h)} = P_{h1}^{c_{h1}} \dots P_{h\mu_h}^{c_{h\mu_h}},$$

wo das Zeichen $=$ für $\sim$ gesetzt werden kann, wenn in allen Faktoren der Koeffizient der höchsten Potenz von x gleich Eins angenommen wird. Dann ist bei Benutzung der schon gebrauchten Bezeichnungen

$$E_t^{(h)} = P_{h1} \dots P_{h\mu_h}$$

und

$$\Phi_t = \prod_{h=0}^{m-1} \prod_{j_h=1}^{\mu_h} P_{hj_h}^{c_{hj_h}},$$

$$\Psi_t = \prod_{h=0}^{m-1} \prod_{j_h=1}^{\mu_h} P_{hj_h},$$

sowie

$$(P_{hj_h}, P_{kj_k}) \sim 1, \ (h \neq k).$$

$P_{hj_h} = 0$ ist eine in Bezug auf (A) irreduzible Teilresolvente $h + 1^{\text{ter}}$ Stufe. Wir nennen auch das Gleichungssystem, das sich aus $P_{hj_h} = 0$ ergibt, wenn

$x = \sum_{h=1}^{m} t_i x_i$ gesetzt wird, sowie die dadurch definierte Mannigfaltigkeit irreduzibel in (A).

Man hat jetzt folgenden Irreduzibilitätssatz:

Ist $V^{(h+1)}$ irgend eine Mannigfaltigkeit $h+1^{\text{ter}}$ Stufe, die durch ein Gleichungssystem mit Koeffizienten aus (A) definiert wird, so sind entweder alle Elemente der in (A) irreduziblen, durch $P_{hj_h} = 0$ definierten Mannigfaltigkeit in $V^{(h+1)}$ enthalten, oder die gemeinsamen Elemente bilden eine Mannigfaltigkeit, deren Stufenzahl größer als $h+1$ ist.

Jedenfalls wird $V^{(h+1)}$ durch ein Gleichungssystem definiert, dessen Gesamtresolvente die Gestalt

$$d_t^{(h)} \ldots d_t^{(m-1)} = 0$$

besitzt; denn $d_t^{(i)}\,(i<h)$ muß gleich Eins sein, weil die Mannigfaltigkeit $V^{(h+1)}$ eben die Stufenzahl $h+1$ hat. Ist $d_t^{(h)}$ durch P_{hj_h} teilbar, so tritt der erste Fall ein; ist dies nicht der Fall, so wird

$$\text{Res.}\begin{pmatrix} d_t^{(h)}, & P_{hj_h} \\ x\ , & 1 \end{pmatrix} = g\,(x_{h+1}, \ldots, x_{m-1}, t_1, \ldots, t_m);$$

dabei ist g von 0 verschieden und der Resultantenbildung gemäß eine lineare Form von $d_t^{(h)}$ und P_{hj_h}. Setzt man also $x = \sum_{i=1}^{m} t_i x_i$, so muß für jedes gemeinsame Element der durch $d_t^{(h)} = 0$ und $P_{hj_h} = 0$ definierten Mannigfaltigkeiten auch

$$g\,(x_{h+1}, \ldots, x_{m-1}, t_1, \ldots, t_m) = 0$$

sein. Dann kann aber die Gesamtresolvente des durch $d_t^{(h)} = 0$, $P_{hj_h} = 0$ gegebenen Gleichungssystems keine Teilresolvente $h+1^{\text{ter}}$ oder noch niedrigerer Stufe enthalten; denn die Existenz einer solchen involviert die Existenz einer Lösung, in welcher $x_{h+1}, \ldots, x_{m-1}$ als Unbestimmte verbleiben, und dies ist eben durch die Relation $g = 0$ ausgeschlossen.

Die weiteren gemeinsamen Elemente sind in den durch $d_i^{(h+1)} = 0, \ldots$ gegebenen Mannigfaltigkeiten enthalten, also jedenfalls Teile von Mannigfaltigkeiten, deren Stufenzahl größer als $h + 1$ ist.

Für Mannigfaltigkeiten m^{ter} Stufe, die aus einer endlichen Anzahl von aus $\{A\}$ entnommenen Wertsystemen bestehn, enthält $V^{(m)}$ entweder alle durch $P_{m-1, j_{m-1}} = 0$ gegebenen Wertsysteme, oder gar keines, da eine Mannigfaltigkeit $V^{(m+1)}$ keinen Inhalt besitzt. In diesem Falle ist eben g eine nicht verschwindende Form der t, und $g = 0$ überhaupt unmöglich. Dieser letzte Fall enthält auch den Irreduzibilitätssatz für Gleichungen mit einer Unbekannten, der als wichtiger Spezialfall noch näher auszuführen ist.

Für eine Gleichung n^{ten} Grades mit einer Unbekannten

$$F(z) = A_0 z^n + A_1 z^{n-1} + \cdots + A_n = 0 \qquad (A_0 \neq 0)$$

bildet man die Gesamtresolvente nach der gegebenen Anweisung, indem man $x = zt$ einführt und mit t^n multipliziert. Diese ist also

$$t^n F\left(\frac{x}{t}\right) = A_0 x^n + A_1 x^{n-1} t + \cdots + A_n t^n = 0.$$

Setzt man hier wieder $x = zt$, so erhält man $t^n F(z) = 0$; für eine einzelne Gleichung geben — wie vorauszusehn war — die auf die Gesamtresolvente bezüglichen Sätze nur eine Tautologie. Nicht so der Irreduzibilitätssatz, der in diesem Falle, da als „Mannigfaltigkeit" nun die sämtlichen Wurzeln einer Gleichung auftreten, die folgende Gestalt erhält:

Ist $G(z) = 0$ irgend eine Gleichung mit Koeffizienten aus (A), so genügen ihr entweder alle Wurzeln der in (A) irreduzibeln Gleichung $F(z) = 0$ oder keine davon*). Dabei bezieht sich selbstverständlich der Begriff der „Wurzel von $F(z) = 0$" auf $\{A\}$.

---

*) Dieser einfachste Irreduzibilitätssatz kann auch ohne die für Gleichungssysteme notwendigen, umständlichen Entwicklungen abgeleitet werden. Ist nämlich $F(z)$ irreduzibel, so hat man entweder $G(z) = F(z) \Phi(z)$, und dann genügt jede Wurzel von $F(z) = 0$ auch der Gleichung

Es ist klar, daß diesem Satze jeder orthoide Bereich, der die Koeffizienten des Gleichungssystems enthält, zu Grunde gelegt werden kann, also insbesondere jeder Bereich (A), der sämtliche Größen aus (A) enthält. Daraus folgt aber eine weitere Formulierung des Irreduzibilitätssatzes, die — im Gegensatze zu den bei Gleichungen mit einer Unbekannten auftretenden Verhältnissen — für Mannigfaltigkeiten, die unendlich viele Elemente enthalten, charakteristisch ist.

Jede Faktorenzerlegung von Φ_t ist — wie wir aus Kap. IV. § 18 wissen — schon in einem bestimmten, aus (A) entstammenden Gattungsbereich (G) ausführbar. Legt man diesen zu Grunde, so wird P_{hj_h} eine absolut irreduzible Form, und $P_{hj_h} = 0$ definiert eine absolut irreduzible Mannigfaltigkeit $h + 1^{\text{ter}}$ Stufe, für welche der folgende Satz gilt:

Eine absolut irreduzible Mannigfaltigkeit $h + 1^{\text{ter}}$ Stufe ist in jeder anderen algebraischen Mannigfaltigkeit $h + 1^{\text{ter}}$ Stufe $V^{(h+1)}$ entweder vollständig enthalten, oder die gemeinsamen Elemente der beiden bilden eine Mannigfaltigkeit, deren Stufenzahl größer als $h + 1$ ist. Jene Mannigfaltigkeit $V^{(h+1)}$ wird durch ein Gleichungssystem definiert, dessen Koeffizienten einem bestimmten Rationalitätsbereiche angehören; adjungiert man diesem die Größen des Gattungsbereichs (G), so erhält man einen orthoiden Bereich, der die Stelle von (A) in dem früher abgeleiteten Irreduzibilitätssatze einnehmen kann, und da P_{hj_h} auch in diesem Bereiche irreduzibel ist, unmittelbar den soeben ausgesprochenen Satz ergibt.

Eine Mannigfaltigkeit $h + 1^{\text{ter}}$ Stufe, d. h. eine $(m - h - 1)$-fache Mannigfaltigkeit wird in geometrischer Auffassungsweise auch ein $(m - h - 1)$fach ausgedehntes Gebilde genannt,

---

$G(z) = 0$; oder die Resultante R von $F(z)$ und $G(z)$ ist von 0 verschieden. Dann zeigt die Relation

$$R = G_1(z)F(z) + F_1(z)G(z),$$

daß für keine Größe z zugleich $F(x)$ und $G(x)$ gleich Null sein können.

dem entsprechend kann der letzte Satz auch noch folgendermaßen ausgedrückt werden:

Es ist unmöglich, einen k-fach ausgedehnten Teil eines absolut irreduziblen k-fach ausgedehnten (algebraischen) Gebildes — insofern dieser „Teil" eben das Gebilde nicht vollständig erschöpft — durch ein algebraisches Gleichungssystem auszudrücken.

Für Mannigfaltigkeiten m^{ter} Stufe, die „0-fach ausgedehnt" sind, geometrisch gesprochen also „aus einer endlichen Anzahl von Punkten" bestehen, verliert der Satz seinen Inhalt. Denn eine absolut irreduzible Mannigfaltigkeit m^{ter} Stufe wird durch eine Gleichung $P_{m-1, j_{m-1}} = 0$ definiert, wo $P_{m-1, j_{m-1}}$ ein Teiler von $D_i^{(m-1)}$ ist. Nun zerfällt aber $D_i^{(m-1)}$ in (G) in lineare Teiler der Gestalt $x - \sum_{i=1}^{m} \xi_i t_i$, wo die Größen ξ_i dem Bereiche (G) angehören und $F_{m-1, j_{m-1}} = 0$ definiert demnach ein einziges Wertsystem $\xi_1, \ldots, \xi_m$, „einen einzelnen Punkt", sodaß der Satz selbstverständlich wird.

§ 8. Sind für das Gleichungssystem $F_j = 0$ Resolventen vorhanden, deren Stufenzahl kleiner als m ist, so genügen diesem unendlich viele Wurzelsysteme, und der Inhalt des Systems kann durch deren vollständige Aufzählung nicht beschrieben werden. Trotzdem kann dieser Inhalt durch eine endliche Reihe algebraischer Größen vollständig charakterisiert werden. Dies geschieht, indem wir statt der durch $D_i^{(h)} = 0$ gegebenen Mannigfaltigkeiten $h + 1^{\text{ter}}$ Stufe jene in endlicher Anzahl vorhandenen „Hauptlösungen $h + 1^{\text{ter}}$ Stufe" in die Betrachtung einbeziehen, in denen wir $x_{h+1}, \ldots, x_{m-1}$ nicht weiter „beliebig" wählen, sondern als Unbestimmte belassen. Auch dann ist $D_i^{(h)}$ als Form von $x, t_1, \ldots, t_m$ nach § 3 in lineare Faktoren zerlegbar, deren Koeffizienten aber nun Größen eines dem Bereiche $((\mathsf{A}), x_{h+1}, \ldots, x_{m-1})$ entstammenden Gattungsbereichs sind. Diese linearen Faktoren haben die Gestalt:

$$x - \sum_{r=1}^{h} \xi_r' t_r - \sum_{s=h+1}^{m-1} x_s t_s - \xi_m' t_m;$$

$\xi_1', \ldots, \xi_h', \xi_{m-1}'$ sind Größen des eben angeführten Bereichs*) und können aus keinem Formbereiche mit weniger Unbestimmten hergeleitet werden, da das als Hauptlösung $h + 1^{\text{ter}}$ Stufe bezeichnete Größensystem jedesmal die Unbestimmten $x_{h+1}, \ldots, x_{m-1}$ selbst enthält.

Die Anzahl der verschiedenen Hauptlösungen $h + 1^{\text{ter}}$ Stufe ist durch die Anzahl der verschiedenen linearen Faktoren von $D_l^{(h)}$ — in der früheren Bezeichnung durch μ_h, den Grad von $E_l^{(h)}$ — gegeben.

Ist P_{hj_h} ein absolut irreduzibler Teiler von $D_l^{(h)}$, und wird diese Größe als Form von $x, t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1}$ aufgefaßt so sind die den linearen Teilern von P_{hj_h} entsprechenden Hauptlösungen konjugierte Lösungen in dem Sinne, daß die aus ihnen zusammengesetzten linearen Formen

$$\sum_{r=1}^{h} \xi_r' t_r + \sum_{s=h+1}^{m-1} x_s t_s + \xi_m' t_m$$

konjugierte Größen sind. Ihre Anzahl ergibt die Ordnung des kleinsten Gattungsbereichs, in dem sie enthalten sind (Kap. IV. § 14—19); diese ist der Grad von P_{hj_h}; wird dieser Grad z. B. mit l bezeichnet, so sind die einzelnen Größen ξ' algebraische Funktionen der Unbestimmten $x_{h+1}, \ldots, x_{m-1}$, deren Ordnung ein Teiler von l ist; jene lineare Form selbst aber ist genau von der Ordnung l. Die soeben angeführten Sätze sind auf Grundlage der an der citierten Stelle gebrauchten Methode leicht einzusehen.

---

*) Daraus folgt — was der späteren Benutzung wegen sogleich bemerkt werden soll — daß aus $D_l^{(h)}$ nach der Substitution $x = \sum_{i=1}^{m} t_i x_i$ die Unbestimmten $t_{h+1}, \ldots, t_{m-1}$ gänzlich herausfallen; denn das gilt für jeden linearen Faktor, also auch für $D_l^{(h)}$. Es wird daher $[D_l^{(h)}]_x = \sum_{i=1}^{m} t_i x_i$ eine Form der x und t mit Ausschluß von $t_{h+1}, \ldots, t_{m-1}$.

Die algebraischen Funktionen von Unbestimmten stehen zu den algebraischen Funktionen von Veränderlichen genau in demselben Verhältnis, wie die Formen zu den ganzen Funktionen. Mit den Hauptlösungen $h + 1^{\text{ter}}$ Stufe sind die linearen Faktoren von $D_t^{(h)}$ vollständig gegeben und damit ist die $D_t^{(h)}$ entsprechende Mannigfaltigkeit prinzipiell bestimmt*).

Die einer absolut irreduzibeln Mannigfaltigkeit $P_{hj_h} = 0$ entsprechenden linearen Faktoren haben in $D_t^{(h)}$ den gleichen Exponenten.

Daß gewisse Wurzelsysteme als Elemente verschiedener Mannigfaltigkeiten zugleich erscheinen können, ist nicht ausgeschlossen; sie sind aber dann in jeder Mannigfaltigkeit besonders zu zählen.

Die Hauptlösungen m^{ter} Stufe sind, wie unmittelbar ersichtlich, Systeme von aus $\{A\}$ entnommenen Größen.

Der Inhalt eines jeden Gleichungssystems ist daher durch die Hauptlösungen, d. h. durch eine Anzahl algebraischer Größen vollständig gegeben. Aber auch dann, wenn die Gesamtheit der einzelnen Lösungen betrachtet wird, ist jede der in diesen Lösungen auftretenden Größen eine algebraische Größe, wie sie schon durch eine Gleichung mit einer Unbekannten definiert wird, wenn man nur die Beschränkung hinzufügt, daß, insofern es möglich ist für eine Anzahl der Unbekannten „beliebige" Größen zu wählen, auch für diese nur algebraische Größen genommen werden sollen. Insofern also keine der Begriffsbildung fremden Elemente hinzugenommen werden, ist das Reich der algebraischen Größen, die durch eine Gleichung mit einer Unbekannten definiert werden, ein in sich geschlossenes, das durch die Hinzunahme von Gleichungssystemen nicht mehr erweitert wird.

Eine Gleichung mit einer Unbekannten ist durch ihre Lösungen und die „Multiplizität" der einzelnen Lösungen — im Sinne der Äquivalenzbestimmung — vollständig gegeben.

*) Wie die Hauptlösungen im einzelnen mit der Darstellung der Mannigfaltigkeit $D_t^{(h)}$ zusammenhängen, wird im nächsten Paragraphen ausführlich erörtert werden.

Wenn $f(x)$ und $g(x)$ dieselben Linearfaktoren mit denselben Exponenten enthalten, so ist $f(x) \sim g(x)$ in Bezug auf den Rationalitätsbereich der Koeffizienten als Äquivalenzbereich.

Es muß schon hier betont werden, daß für Gleichungssysteme die Verhältnisse wenigstens nicht immer ebenso liegen. Es gibt Gleichungssysteme, die dieselbe Gesamtresolvente besitzen und sich trotzdem nicht vollständig ersetzen können. Um hierfür ein einfaches Beispiel anzuführen, haben die beiden Systeme

$$(x_1 + x_2)^2 = 0,\ x_1 - x_2 = 0 \qquad \text{(I.)}$$

und

$$(x_1 - x_2)^2 = 0,\ x_1 + x_2 = 0 \qquad \text{(II.)}$$

dieselbe Gesamtresolvente $x^2 = 0$, d. h. das einzige doppelt zu zählende Wurzelsystem $(0, 0)$. Trotzdem kommt es keineswegs auf dasselbe hinaus, ob man der Gleichung $x_1 + x_2 = 0$ das System (I) oder (II) hinzufügt. Im zweiten Falle bleibt die Gesamtresolvente $x^2 = 0$; im ersten Falle wird sie $x = 0$*).

---

*) Der eigentliche Grund für das Auftreten solcher Ausnahmefälle liegt darin, daß die Gesamtheit der aus $\{A\}$ genommenen Wurzelsysteme der Gleichungen $F_i = 0$, der „Inhalt" dieses Systems, zu seiner Charakterisierung nicht genügt. Um dies zu erreichen, muß man auch unendlich kleine Größen in den Kreis der Betrachtung einbeziehen. Wie schon erwähnt (Kap. IV. § 9), braucht man dabei den Boden der arithmetisch-algebraischen Methoden nicht zu verlassen. Darauf soll allerdings in diesem Buche nicht eingegangen werden; indem ich mir eine ausführliche Darstellung vorbehalte, soll jedoch im Anschluß an das Beispiel des Textes das Wesen der Sache in diesem einfachsten Falle dargelegt werden.

Sei (A) der zu Grunde liegende orthoide Bereich, $a_1, a_2, \ldots, b_1, b_2, \ldots$ irgend welche Größen des Bereichs, δ ein neues Symbol, das als unendlich kleine Größe erster Ordnung bezeichnet werden soll. Dann bilden die „Größen"

$$a_1 + b_1\delta,\ a_2 + b_2\delta, \ldots,$$

deren Additions- und Multiplikationsgesetz durch

$$(a_1 + b_1\delta) + (a_2 + b_2\delta) = a_1 + a_2 + (b_1 + b_2)\delta$$

$$(a_1 + b_1\delta)(a_2 + b_2\delta) = a_1 a_2 + (a_1 b_2 + a_2 b_1)\delta$$

Die Hauptdarstellungen reiner Mannigfaltigkeiten.

§ 9. Irgend eine wie immer gegebene (algebraische) reine Mannigfaltigkeit $h+1^{\text{ter}}$ Stufe $V^{(h+1)}$ wird schließlich nach Ausführung einer gewissen linearen Transformation dem Vorhergehenden gemäß immer durch eine Form

$$\varphi(x; t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1})$$

in der Weise charakterisiert, daß, wenn $E_t^{(h)} = 0$ eine reduzierte vollständige Resolvente $h+1^{\text{ter}}$ Stufe, φ ein Teiler von $E_t^{(h)}$ ist und

$$[\varphi]_{x=\sum_{i=1}^{m} x_i t_i} = 0$$

in kurzer Zusammenfassung jenes Gleichungssystem darstellt, dessen Inhalt sämtliche Elemente der Mannigfaltigkeit $V^{(h+1)}$ und nur diese umfaßt. Dabei ist nach Potenzprodukten der t zu ordnen und der Koeffizient jedes einzelnen Potenzproduktes gleich Null zu setzen.

Ist also $x_1, \ldots, x_m$ ein Element von $V^{(h+1)}$, so wird φ für $x = \sum x_i t_i$ immer identisch gleich Null, und dasselbe muß für die Derivierte nach $t_1, \ldots, t_m$ der Fall sein.

Setzt man also

$$\frac{\partial \varphi}{\partial x} = \varphi_0, \quad \frac{\partial \varphi}{\partial t_i} = \varphi_i$$

und benutzt die eckige Klammer schon ohne den Zusatz $x = \sum x_i t_i$ als Zeichen dieser Substitution, so wird auch

$$[\varphi_0] x_i + [\varphi_i] = 0.$$

---

gegeben sind, einen hyperorthoiden Bereich, der als dem Bereiche (A) entstammender Infinitesimalbereich erster Ordnung bezeichnet werden kann. (Dabei hat man es in Wirklichkeit nur mit den Größenpaaren $(a_1, b_1), \ldots$ zu tun, und die Schreibweise $a_1 + b_1 \delta$ wird nur aus Bequemlichkeitsgründen eingeführt, δ bezeichnet das Größenpaar $(0, 1)$).

Nun haben aber die Systeme (I) und (II) nicht mehr denselben Inhalt. Dem Systeme (I) genügt jedes Größensystem $x_1 = a\delta$, $x_2 = a\delta$; dem Systeme (II) jedes Größensystem $x_1 = -a\delta$, $x_2 = a\delta$, wo a eine beliebige Größe aus (A). Sowohl (I) wie (II) genügen unendlich viele Wurzelsysteme, die alle der Lösung $(0, 0)$ „unendlich nahe" liegen. Gemeinsam ist aber nur das eine Wurzelsystem $(0, 0)$.

Da φ keine mehrfachen Teiler hat, wird die Discriminante von φ nach x eine nicht verschwindende Form von $t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1}$ und man kann in beliebiger Anzahl Wertsysteme

$$t_i = a_i, \quad a_m \neq 0,$$

bestimmen, so daß die Discriminante von

$$\varphi(x; a_1, \ldots, a_m, x_{h+1}, \ldots, x_{m-1})$$

eine von 0 verschiedene Form der $x_{h+1}, \ldots, x_{m-1}$ wird. Diese sei $\Delta_a(x_{h+1}, \ldots, x_{m-1})$.

Dann erhalten wir in

$$\begin{aligned} [\varphi]_a &= \varphi(x, a_1, \ldots, a_m, x_{h+1}, \ldots, x_{m-1}) = 0 \\ [\varphi_0]_a x_i + [\varphi_i]_a &= 0, \qquad (i = 1, \ldots, h) \end{aligned} \tag{I.}$$

wo das Symbol $[\cdots]_a$ die Ausführung der Substitutionen $t_i = a_i$ andeutet, eine Hauptdarstellung der Mannigfaltigkeit $V^{(h+1)}$ in $h+1$ Gleichungen, für welche jedoch die darin enthaltene durch $\Delta_a = 0$ bestimmte Mannigfaltigkeit von wenigstens*) $h + 2^{\text{ter}}$ Stufe eine Ausnahmestellung einnehmen kann.

Denn ist $x_1, x_2, \ldots, x_m$ irgend ein Element der Mannigfaltigkeit $V^{(h+1)}$, für welches Δ_a von 0 verschieden ist, so muß, da die Zerlegung von φ in lineare Faktoren auch für $t_i = a_i$ erhalten bleibt, unter den Wurzeln von $[\varphi]_a = 0$, wenn $x_{h+1}, \ldots, x_{m-1}$ als die entsprechenden Koordinaten eines Elementes von $V^{(h+1)}$ angenommen werden,

$$x = \sum_{i=1}^{m} a_i x_i$$

sich befinden, und da nun $\left[\frac{\partial \varphi}{\partial x}\right]_a = [\varphi_0]_a$ für $[\varphi]_a = 0$ nicht verschwindet, vermöge der Gleichungen in der zweiten Zeile aus $x, x_{h+1}, \ldots, x_{m-1}$ sich $x_1, \ldots, x_h$ und schließlich aus

*) Der Zusatz „wenigstens" ist deshalb einzuschalten, weil es vorkommen kann, daß Δ_a überhaupt kein x enthält; in diesem Falle hat die Gleichung $\Delta_a = 0$ überhaupt „keinen Inhalt".

$$x = \sum_{i=1}^{m} a_i x_i \quad \text{oder} \quad [\varphi_0]_a x_m + [\varphi_m]_a = 0$$

auch x_m eindeutig ergeben. Umgekehrt ist auch jede Wurzel von $[\varphi]_a = 0$ von der Form $x = \sum a_i x_i$, wo $x_1, \ldots, x_m$ ein Element von $V^{(h+1)}$; jede Lösung von (I.) ergibt daher ein Element von $V^{(h+1)}$ und umgekehrt, insofern die in $\Delta_a = 0$ enthaltenen Elemente ausgeschlossen sind.

Mit Rücksicht auf die Ausnahmestellung der Elemente $\Delta_a = 0$ kann jene Hauptdarstellung in zweierlei Weise interpretiert werden.

a) Die Gleichungen (I.) mit Hinzufügung der Bedingung $\Delta_a \neq 0$ ergeben eine Hauptdarstellung von $V^{(h+1)}$, welche deren Elemente — mit Ausschluß einer ausgezeichneten Mannigfaltigkeit von wenigstens $h + 2^{\text{ter}}$ Stufe $W^{(h+2)}$ — vollständig und ausschließlich ergibt. Diese ausgeschlossene ausgezeichnete Mannigfaltigkeit setzt sich aus zwei Teilen von ganz verschiedenem Charakter zusammen. Die Mannigfaltigkeit $V^{(h+1)}$ kann eine singuläre Mannigfaltigkeit (siehe den Schluß von § 6) besitzen, und diese ist, da für sie eben Δ_a bei jeder Wahl der a verschwindet, jedenfalls in $W^{(h+2)}$ enthalten. Im Gegensatz zu diesen singulären Elementen ist das Auftreten irgend eines weiteren Elementes von $W^{(h+2)}$ von der Wahl der a abhängig, also in geometrischer Ausdrucksweise, da $x = \sum a_i x_i$ eine Koordinatentransformation ausdrückt, eine Folge der speziellen Wahl des Koordinatensystems. Denn sobald die Discriminante von $\varphi(x, t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1})$ nach x nicht identisch Null ist, kann man auch ein Wertsystem $t_i = a_i$ bestimmen, für welches dies nicht der Fall ist.

b) Die Gleichungen (I.) ohne weitere beschränkende Bedingung ergeben alle Elemente der Mannigfaltigkeit $V^{(h+1)}$, aber außerdem noch alle Elemente von $(x_1, \ldots, x_m)$, für welche $\Delta_a(x_{h+1}, \ldots, x_{m-1}) = 0$ und dann weiter $x_1, \ldots, x_h$ beliebig gewählt sind, während sich x_m aus $x = \sum a_i x_i$ ergibt, wo x irgend eine mehrfache Wurzel der Gleichung $[\varphi]_a = 0$ be-

deutet. Die so charakterisierten Elemente bestimmen, wie man unmittelbar sieht, eine Mannigfaltigkeit zweiter Stufe.

Soweit nämlich $\Delta_a \neq 0$, stehen die Verhältnisse ebenso wie früher; dasselbe ist auch dann der Fall, wenn zwar $\Delta_a = 0$, aber x nur eine einfache Wurzel von $[\varphi]_a = 0$ ist. Ist aber $\Delta_a = 0$ und x eine mehrfache Wurzel von $[\varphi]_a = 0$, so ist jedenfalls auch $[\varphi_0]_a = 0$ und die Gleichungen (I.) können nur dann befriedigt sein, wenn auch:

$$[\varphi_i]_a = 0, \quad (i = 1, \ldots, h).$$

Da aber auf das ursprüngliche Gleichungssystem schon eine entsprechende lineare Transformation ausgeübt wurde, hat die darzustellende Mannigfaltigkeit jedenfalls ein Element, das den jetzt festgelegten Werten von $x, x_{h+1}, \ldots, x_m$ entspricht. Die diesem Elemente entsprechenden Werte von $x_1, \ldots, x_h$ müssen aber unbedingt den in der zweiten Zeile von (I.) stehenden Gleichungen genügen, d. h. aus $\Delta_a = 0$ und $[\varphi_0]_a = 0$ folgt immer auch $[\varphi_i]_a = 0$, $(i = 1, \ldots, h)$. Es bleibt also nur die Gleichung in der ersten Zeile von (I.), und es ergibt sich insgesamt also eine Beschränkung der freien Veränderlichkeit von $(x_1, \ldots, x_m)$ durch 2 Gleichungen, von denen die eine x_{h+1}, die andere x_m durch die anderen x bestimmt. Ist Δ_a nicht regulär in Bezug auf x_{h+1}, so hat man wieder nur vorher eine lineare Transformation auszuführen.

Um ein kurzes Beispiel anzuführen, seien für eine reine algebraische Raumkurve sogleich x, x_1, x_2 die gewöhnlichen Cartesischen Koordinaten; dann wird ihre Hauptdarstellung — die a auch schon als spezielle Zahlen verstanden — die folgende

$$\varphi(x, x_2) = 0$$
$$\varphi_0(x, x_2)\, x_1 + \varphi_1(x, x_2) = 0,$$

wo φ_0 und φ nur für jene Wertsysteme zugleich verschwinden, für welche die Discriminante von φ nach x und auch $\varphi_1(x, x_2)$ Null wird. In diese Hauptdarstellung der algebraischen Raumkurve treten demnach eine endliche Anzahl paralleler Geraden als überflüssige Elemente ein.

§ 10. In gewissen Fällen ergibt die Hauptdarstellung doch schon die vollständige und ausschließliche Darstellung der gegebenen Mannigfaltigkeit; insbesondere ist dies der Fall für jede in $(x_1, \ldots, x_m)$ enthaltene reine Mannigfaltigkeit erster und m^{ter} Stufe. Man hat die Sätze:

Jede reine Mannigfaltigkeit erster Stufe wird durch den Inhalt *einer* Gleichung vollständig und ausschließlich gegeben.

Bei Wiederholung der Schlüsse des § 9 für diesen Fall bleiben nämlich die Gleichungen zweiter Art aus (I.) ganz fort. — Dasselbe Resultat ergibt sich auch daraus, daß — nach der ersten Note zu § 8 — D_t nach der Substitution $x = \sum_{i=1}^{m} t_i x_i$ eine homogene Form von t_m wird, also die Gestalt $t_m^k \Phi$ annimmt, dasselbe also auch für jeden Teiler von D_t stattfindet, so daß sich als vollständige Definition der entsprechenden Mannigfaltigkeit erster Stufe die Gleichung $\varphi = 0$ ergibt.

Ferner ergibt sich der Satz:

Jede Mannigfaltigkeit m^{ter} Stufe aus $(x_1, \ldots, x_m)$, d. h. die in endlicher Anzahl vorhandenen Wertsysteme

$$\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk} \qquad (k = 1, 2, \ldots, N)$$

werden durch den Inhalt eines Systems von m Gleichungen vollständig und ausschließlich gegeben.

Denn jene mit Δ_a bezeichnete Discriminante ist jetzt eine von 0 verschiedene Größe, die kein x weiter enthält, und es sind demnach in diesem Falle keinerlei singuläre oder ausgezeichnete Elemente vorhanden.

Ist $0 < h < m - 1$, so können die Gleichungen (I.) außer $V^{(h+1)}$ noch eine Mannigfaltigkeit zweiter Stufe ergeben. Diese kann aber auch wegfallen, wenn Δ_a eine von den x unabhängige (und selbstverständlich von 0 verschiedene) Größe ist.

Trotz des Auftretens jener Mannigfaltigkeit zweiter Stufe ist man berechtigt, die Gleichungen (I.) als Darstellung von $V^{(h+1)}$ in Anspruch zu nehmen, denn sie bestimmen diese vollständig. Bildet man nämlich die vollständige Resolvente

des Systems (I.), so muß diese neben der Teilresolvente zweiter Stufe auch die Resolvente $h + 1^{\text{ter}}$ Stufe ergeben, die $V^{(h+1)}$ vollständig und ausschließlich definiert. Denn (I.) ergibt nur jene Mannigfaltigkeiten, die sich gesondert ergeben müssen, weil ihre gemeinschaftlichen Elemente eine Mannigfaltigkeit von wenigstens $h + 2^{\text{ter}}$ Stufe ergeben.

Wie der Begriff der Hauptdarstellung einer $V^{(h+1)}$ sich naturgemäß erweitert, liegt auf der Hand. Als solche wird jedes System von $h + 1$ Gleichungen zu betrachten sein, das alle Elemente von $V^{(h+1)}$ und nur diese definiert, wenn alle Elemente einer solchen Mannigfaltigkeit erster Stufe $\psi = 0$ ausgeschlossen sind, deren mit $V^{(h+1)}$ gemeinsamen Elemente eine Mannigfaltigkeit von wenigstens $h + 2^{\text{ter}}$ Stufe bilden*).

Noch sei kurz der aus dieser Darstellung sich ergebende Fundamentalsatz für die „Theorie der Abbildung" erwähnt**):

Jede reine Mannigfaltigkeit $V^{(h+1)}$, die einer beliebigen Mannigfaltigkeit $(x_1, \ldots, x_m)$ entnommen ist, läßt sich mit einer Mannigfaltigkeit erster Stufe, die der $(m - h)$-fach ausgedehnten Mannigfaltigkeit $(z_1, z_2, \ldots, z_{m-h})$ entnommen ist, in gegenseitig eindeutige Beziehunng bringen, die nur für eine in $V^{(h+1)}$ enthaltene Mannigfaltigkeit von wenigstens $h + 2^{\text{ter}}$ Stufe Ausnahmen erleiden kann.

Betrachtet man $x, x_{h+1}, \ldots, x_{m-1}$ als unabhängige Veränderliche, so steht die in $(x, x_{h+1}, \ldots, x_{m-1})$ gelegene Mannigfaltigkeit erster Stufe $[\varphi]_a = 0$ mit $V^{(h+1)}$ in der angegebenen ein-eindeutigen Beziehung, die geradezu durch die Gleichungen (I.) gegeben ist, denen man noch der Vollständigkeit wegen die daraus sich weiter ergebende Gleichung

$$[\varphi_0]_a x_m + [\varphi_m]_a = 0$$

hinzufügen kann.

---

*) Die Bezeichnung als Hauptdarstellung (figuration principale) rührt von Molk her, in dessen schon früher citierter Abhandlung (auf Seite 153) man eine „Hauptdarstellung" im jetzt gegebenen Sinne des Wortes findet.

**) Kronecker, Festschrift, § 10.

Die vollständige Darstellung beliebiger Mannigfaltigkeiten durch $m + 1$ Gleichungen.

§ 11. Wir gehen zur Entwicklung des folgenden von Kronecker ohne Beweis gegebenen fundamentalen Satzes über*):

Der Inhalt eines beliebigen Systems von Gleichungen $F_j = 0$ $(j = 1, \ldots, k)$ mit den Unbekannten $x_1, \ldots, x_m$ kann vollständig und ausschließlich durch ein System von höchstens $m + 1$ Gleichungen gegeben werden.

Da der Satz von einer auf die Unbekannten ausgeübten linearen Transformation mit von 0 verschiedener Determinante unabhängig ist, kann das vorgelegte System $F_j = 0$ wieder in der bisherigen Weise als von Zufälligkeiten befreit angesehen werden. Da es sich aber ausschließlich um den Inhalt des Gleichungssystems handelt, kann vor allem die reduzierte Resolvente des Systems (§ 7)

$$\Psi_t = \prod_{h=0}^{m-1} \prod_{j_h=1}^{\mu_h} P_{hj_h} = 0$$

zu Grunde gelegt und dann noch weiter vorausgesetzt werden, daß die in bekannter Weise durch

$$P_{hj_h} = 0$$

definierte Mannigfaltigkeit, die einen Teil des darzustellenden Inhalts ausmacht, nicht schon in der durch

$$P_{kj_k} = 0 \qquad (k < h)$$

definierten Mannigfaltigkeit vollständig enthalten ist; denn in diesem Falle stellt schon $\Psi_t = 0$ nach Entfernung des Faktors P_{hj_h} den Inhalt von $F_j = 0$ vollständig dar. Um zu ent-

*) Kronecker, Festschrift, § 10.

scheiden, ob ein P_{hj_h} für die Darstellung des Inhalts in dieser Weise überflüssig wird, hat man nur die durch

$$P_{kj_k} = 0, \quad P_{hj_h} = 0 \tag{P}$$

zusammengesetzten Gleichungssysteme zu betrachten. Ein solches System (P) stellt wegen $P_{hj_h} = 0$ eine Mannigfaltigkeit dar, deren Stufenzahl wenigstens $h + 1$ ist. Bildet man demnach die Gesamtresolvente des Systems (P), so wird in dieser die vollständige Teilresolvente, deren Stufenzahl die kleinste ist, entweder von der $h + 1^{\text{ten}}$ oder von höherer Stufe sein. Im ersten Falle muß also die durch diese Resolvente definierte Mannigfaltigkeit die Mannigfaltigkeit $P_{hj_h} = 0$, da diese irreduzibel ist, vollständig enthalten und der Inhalt von $P_{hj_h} = 0$ ist im Inhalte von $P_{kj_k} = 0$ vollständig enthalten. Im zweiten Falle bilden die gemeinsamen Elemente von $P_{kj_k} = 0$ und $P_{hj_h} = 0$ eine Mannigfaltigkeit von höchstens $h + 2^{\text{ter}}$ Stufe und $P_{kj_k} = 0$ enthält nur eine $V^{(h+2)}$ aus $P_{hj_h} = 0$.

Nachdem so für jedes P_{hj_h} entschieden wurde, ob es für die vollständige Darstellung des Inhalts von $F_j = 0$ beizubehalten ist, erhält man diesen aus dem durch

$$\psi = \prod_{h=0}^{m-1} \prod_{j_h=1}^{\nu_h} Q_{hj_h} = 0$$

dargestellten Gleichungssystem, wo die Elemente, die den durch

$$Q_{kj_k} = 0, \quad Q_{hj_h} = 0, \qquad (k < h)$$

definierten Mannigfaltigkeiten gemeinsam sind, eine Mannigfaltigkeit von $h + 2^{\text{ter}}$ oder höherer Stufe bilden.

Auch die Gleichung

$$\psi(x, x_1, \ldots, x_{m-1}, t_1, \ldots, t_m) = 0$$

ist eine Resolvente des Systems $F_j = 0$; insofern der Inhalt des Systems, welches man erhält, indem man die Koeffizienten der Potenzprodukte $t_m^{a_m}, \ldots, t_1^{a_1}$ einzeln gleich Null setzt, mit dem Inhalt des Systems $F_j = 0$ vollständig übereinstimmt. Sie kann als Minimalresolvente des Systems $F_j = 0$ be-

zeichnet werden, weil jede Zusammenfassung des Inhalts von $F_j = 0$ in einer Reihe von Mannigfaltigkeiten erster, zweiter Stufe u. s. f. die durch die Minimalresolvente gegebenen Mannigfaltigkeiten unbedingt enthalten muß. Wäre $V^{(h+1)}$ die erste irreduzible Mannigfaltigkeit des Systems $F_j = 0$, die nicht auch durch $\psi = 0$ gegeben ist, so müßte sie in einer Mannigfaltigkeit niedrigerer Stufe aus $\psi = 0$ vollständig enthalten sein, und wäre für die Angabe des Inhalts von $F_j = 0$ ganz überflüssig. Dem gegenüber ist die Aufzählung jeder Mannigfaltigkeit, die sich aus $\psi = 0$ ergibt, notwendig; denn die mit einer andern Mannigfaltigkeit aus $\psi = 0$ gemeinsamen Elemente ergeben nur eine Mannigfaltigkeit von höherer Stufenzahl.

Daraus ist auch ersichtlich, daß zwei Gleichungssysteme dann und nur dann denselben Inhalt besitzen, wenn ihre Minimalresolventen dieselben sind.

Jene Minimalresolvente mag noch, um für das Folgende eine kürzere Fassung zu erlangen,

$$\psi = \psi^{(0)}\,\psi^{(1)} \ldots \psi^{(m-1)}$$

geschrieben werden, wo

$$\psi^{(h)} = \prod_{j_h=1}^{r_h} Q_{hj_h}$$

ist.

Man beweist nun leicht den folgenden Satz:

Sei $F_j = 0$, $(j = 1, \ldots, k)$ ein Gleichungssystem mit der Minimalresolvente $\psi = 0$. Sei ferner

$$G_r^{(h)} = 0, \quad (r = 1, \ldots, h) \qquad (\Sigma_{h+1})$$

ein Gleichungssystem, dessen Inhalt den Inhalt des Systems $F_j = 0$ vollständig umfaßt und außer diesem nur Mannigfaltigkeiten von $h + 1^{\text{ter}}$ oder höherer Stufe enthält. Dann kann man immer Systeme von Größen (auch rationale und ganze Zahlen) $a_1, \ldots, a_m$ so bestimmen, daß das System

$$[\psi]_{x=\sum a_i x_i} = 0, \quad G_r^{(h)} = 0, \quad (r = 1, \ldots, h), \qquad (\Sigma_{h+2})$$

dessen Inhalt den Inhalt des Systems $F_j = 0$ wieder vollständig umfaßt, außer diesem nur mehr Mannigfaltigkeiten von $h + 2^{\text{ter}}$ oder höherer Stufe enthält.

Berücksichtigt man die jetzt geltenden Festsetzungen und die Eigenschaften der Minimalresolvente, so erhält man für die Minimalresolvente des Systems (Σ_{h+1}) jedenfalls folgende Gestalt:

$$\varrho_{h+1} = \psi^{(0)} \psi^{(1)} \ldots \psi^{(h-1)} \chi^{(h)} \ldots \chi^{(m-1)} = 0,$$

wo noch $\chi^{(h)}$ durch $\psi^{(h)}$ teilbar ist. Ist nun $\chi^{(h)} \sim \psi^{(h)}$, so wird unser Satz — wie unmittelbar zu sehen — bei jeder Wahl der Größen a richtig sein.

Im entgegengesetzten Falle ist

$$\chi^{(h)} = \psi^{(h)} \chi_1^{(h)},$$

und $\chi^{(h)}$ nicht ~ 1. Die irreduzibeln Teiler von $\chi_1^{(h)}$ und $\psi^{(h)}$ sind durchweg verschieden. Ist nun $\pi^{(h)}$ irgend ein irreduzibler Teiler von $\chi_1^{(h)}$, so kann $\pi^{(h)} = 0$ nach der Definition der Minimalresolvente mit keiner Mannigfaltigkeit $\psi^{(j)} = 0$ eine Mannigfaltigkeit gemeinsam enthalten, deren Stufenzahl kleiner als $h + 2$ ist. Es gibt daher Größen $x_i = \xi_i$, die einem bestimmten aus (A) entstammenden Gattungsbereiche angehören, für die $[\pi^{(h)}] = 0$ wird, während $[\psi]$ von 0 verschieden ist und also auch von 0 verschieden bleibt, wenn man an Stelle der t gewisse Größensysteme $a_1, \ldots, a_m$ setzt (die auch aus rationalen und ganzen Zahlen gewählt werden können). Dann wird aber die Minimalresolvente $\varrho_{h+2} = 0$ des Systems (Σ_{h+2}) in der Tat dem zu beweisenden Satze entsprechen. Es sind $\psi^{(0)}, \psi^{(1)}, \ldots, \psi^{(h)}$ Teiler von ϱ_{h+2}; dagegen kann $\pi^{(h)}$ wegen des Hinzutretens der Gleichung $[\psi]_{x = \Sigma a_i x_i} = 0$ kein solcher sein und ebensowenig, wenn nur die Größen $a_1, \ldots, a_m$ passend gewählt sind, irgend ein anderer irreduzibler Teiler von $\chi_1^{(h)}$. Endlich kann auch keine weitere Mannigfaltigkeit $h + 1^{\text{ter}}$ oder niedrigerer Stufe dem System (Σ_{h+2}) genügen, da diese dann auch dem System (Σ_{h+1}) genügen müßte.

Nun kann man aber von einer Gleichung $[\psi]_{x = \Sigma a_i x_i} = 0$

als System (Σ_1) ausgehen und erhält dann schließlich das Gleichungssystem:

$$\psi(\Sigma a_{ri} x_i, x_1, \ldots, x_{m-1}, a_{r1}, \ldots, a_{rm}) = 0, \quad (r = 1, \ldots, k) \qquad (S_k)$$

dessen Minimalresolvente mit der des Systems $F_j = 0$ übereinstimmt. Dann ist aber auch der Inhalt der beiden Systeme derselbe. Die Anzahl der Gleichungen in (S_k) ist dem zu Beginn dieses Paragraphen ausgesprochenen Satze gemäß $\leqq m + 1$. Der Inhalt des Systems (S_k), in dem die Anzahl der Gleichungen k ist, kann sich von dem Inhalte des Systems $F_j = 0$ nur mehr durch Mannigfaltigkeiten k^{ter} oder höherer Stufe unterscheiden, im Falle $k = m + 1$ also nur mehr durch „Mannigfaltigkeiten $m + 1^{\text{ter}}$ Stufe", die eben gar keinen Inhalt mehr besitzen*).

Gleichungssysteme, deren Inhalt eine lineare Mannigfaltigkeit bildet.

§ 12. Eine lineare Mannigfaltigkeit ist eine solche, die durch ein System linearer Gleichungen definiert wird.

Man erkennt leicht, welche Gestalt die Gesamtresolvente eines Systems linearer Gleichungen:

$$c_{i1} x_1 + c_{i2} x_2 + \cdots + c_{im} x_m + c_{i,m+1} = 0 \quad (i = 1, 2, \ldots, k); \qquad (1.)$$

besitzt. Die Transformation

$$x = t_1 x_1 + t_2 x_2 + \cdots + t_m x_m$$

gibt ihm die Gestalt

$$x - x_1 t_1 - \cdots - x_{m-1} t_{m-1} - X_{im} t_m = 0 \quad (i = 1, 2, \ldots, k), \qquad (2.)$$

*) Vahlen hat an einem schönen Beispiele gezeigt, daß es in der Tat Fälle gibt, wo der Inhalt eines Gleichungssystems mit m Unbekannten nicht durch weniger als $m + 1$ Gleichungen darstellbar ist („Bemerkung zur vollständigen Darstellung algebraischer Raumkurven", Journal f. r. u. a. Mathematik, Bd. 108, pag. 346.).

wo X_{im} eine lineare Form von $x_1, \ldots, x_{m-1}$ bedeutet und man mit den Koeffizienten von x_m, den Größen c_{im}, dividieren konnte, wenn, wie wir immer voraussetzen, die linken Seiten der Gleichungen, eventuell nach einer passenden linearen Transformation, reguläre Formen sind. Da wir es aber mit linearen Formen zu tun haben, können nur die folgenden zwei Fälle eintreten. Entweder sind die linken Seiten der Gleichungen (2.) durchweg äquivalente Formen; also irgend eine davon die vollständige Teilresolvente erster Stufe $D_t = 0$; dann sind aber die (nach Kap. III. § 18 zu bildenden) $\overline{F}_j$ mit 1 äquivalent und $D_t = 0$ ist auch die Gesamtresolvente. Oder es ist $D_t \sim 1$ und die Formen $\overline{F}_j$ sind die auf der linken Seite in (2.) stehenden Formen. Dann ist die Resultante von

$$\sum_{i=1}^{k} u_i (x - x_1 t_1 - \cdots - x_{m-1} t_{m-1} - X_{im} t_m)$$

und

$$\sum_{i=1}^{k} u_1' (x - x_1 t_1 - \cdots - x_{m-1} t_{m-1} - X_{im} t_m)$$

nach x zu bilden und die Koeffizienten der Potenzprodukte der u und u' sind die Formen $F_{j_1}^{(1)}$. Man erkennt unmittelbar, daß jene Resultante, also auch die Formen $F_{j_1}^{(1)}$ lineare Formen von $x, x_2, \ldots, x_{m-1}$ sind. Diese sind wieder entweder durchweg äquivalente Formen und dann gibt irgend eine von ihnen wie früher die Gesamtresolvente des Systems $D_i^{(1)} = 0$; oder aber es ist $D_i^{(1)} \sim 1$. In ähnlicher Weise weiter gehend, erkennt man, daß das System linearer Gleichungen entweder überhaupt keinen Inhalt besitzt oder aber eine Gesamtresultante von der Gestalt

$$x - X_1 t_1 - \cdots - X_h t_h - x_{h+1} t_{h+1} - \cdots - x_{m-1} t_{m-1} - X_m t_m = 0 \qquad (\Lambda)$$

besitzt, wo $X_1, \ldots, X_h, X_m$ lineare Formen von $x_{h+1}, \ldots, x_{m-1}$ sind. Denn die auf der linken Seite stehende Form muß nach den letzten Erörterungen eine lineare Form von $x, x_{h+1}, \ldots, x_{m-1}$ und als vollständige Teilresolvente $h + 1^{\text{ter}}$ Stufe eine

homogene Form von $x, t_1, \ldots, t_m$ sein, in welcher der Koeffizient der höchsten Potenz von x die t nicht enthält (§ 4 dieses Kapitels). Die betrachtete Form ist also auch in Bezug auf die Reihe der Unbestimmten $x, t_1, \ldots, t_m$ linear.

Es ist (Λ) auch die Minimalresolvente des Systems (1.), wenn dieses überhaupt einen Inhalt besitzt, und zugleich hat man in diesem Falle (1.) nach einer eventuell notwendigen linearen Transformation auf die „einfachste" Gestalt

$$x_i = X_i, \quad x_m = X_m \qquad (i = 1, \ldots, h) \qquad (\Lambda_1)$$

gebracht.

Da nun zwei Gleichungssysteme nur dann denselben Inhalt besitzen, wenn ihre Minimalresolventen übereinstimmen, so hat man den Satz:

Der Inhalt eines beliebigen Gleichungssystems bildet dann und nur dann eine lineare Mannigfaltigkeit, wenn die Minimalresolvente die Gestalt (Λ) besitzt, und diese lineare Mannigfaltigkeit ist dann durch rationale Operationen in der Gestalt (Λ_1) bestimmt.

Dabei ist noch der Fall des homogenen linearen Systems hervorzuheben. Man sieht unmittelbar, daß eine lineare Mannigfaltigkeit dann und nur dann durch ein homogenes lineares System definiert wird, wenn diese das Element $x_i = 0$ $(i = 1, \ldots, m)$ enthält.

§ 13. Der Inhalt eines Gleichungssystems „bildet eine Schar in $\{A\}$", wenn mit $(\xi'_1, \ldots, \xi'_m)$ und $(\xi''_1, \ldots, \xi''_m)$ immer auch $(u\xi'_1 + v\xi''_1, \ldots, u\xi'_m + v\xi''_m)$ bei beliebigen Werten von u und v ein Wurzelsystem ist.

Die beiden (trivialen) Grenzfälle, wo das Gleichungssystem keinen Inhalt besitzt oder aber keine Beschränkungen der Veränderlichkeit von $x_1, \ldots, x_m$ statuiert, sollen dabei im folgenden schon als ausgeschlossen betrachtet werden.

Die k Wurzelsysteme

$$\xi_{1j}, \xi_{2j}, \ldots, \xi_{mj} \qquad (j = 1, \ldots, k;\ k \leqq m)$$

sollen „voneinander unabhängig" heißen, wenn die aus der Matrix

$$|\xi_{ij}|_{(i=1,\ldots,m;\ j=1,\ldots,k)}$$

gebildeten Determinanten k^{ten} Grades nicht sämtlich verschwinden.

Ein wirkliches Gleichungssystem, d. h. ein solches, das in der Tat die Veränderlichkeit von $x_1, \ldots, x_m$ beschränkt, also nicht durchweg aus Identitäten besteht, kann, wenn sein Inhalt eine Schar in $\{A\}$ bildet, nicht mehr als $m - 1$ Wurzelsysteme besitzen, die voneinander unabhängig sind. Denn bei m unabhängigen Wurzelsystemen würde in den Gleichungen

$$x_i = \sum_{j=1}^{m} u_j \xi_{ij} \qquad (j = 1, \ldots, m)$$

die Determinante $|\xi_{ij}|$ nicht verschwinden, also für beliebige x_i ein System von Werten u_i bestimmt werden können, das den Gleichungen genügt. Da aber nach der Definition der Schar das Wertsystem $(x_1, \ldots, x_m)$ dann ein Wurzelsystem ist, so müßte das Gleichungssystem durchweg aus Identitäten bestehen.

Wenn der Inhalt des vorgelegten Gleichungssystems eine Schar in $\{A\}$ bildet, gibt es demnach eine bestimmte nicht negative, ganze Zahl k, die kleiner als m ist, von der Beschaffenheit, daß es genau k, aber nicht mehr voneinander unabhängige Wurzelsysteme gibt. Die Schar soll in diesem Falle eine k-gliedrige Schar genannt werden. (Der Fall $k = 0$ entspricht einem System, welches nur die einzige Lösung $x_i = 0$ besitzt.)

Ist die Schar eine k-gliedrige und sind

$$\xi_{1j}, \ldots, \xi_{mj} \qquad (j = 1, \ldots, k)$$

k voneinander unabhängige Wurzelsysteme, ferner $x_1, \ldots, x_m$ irgend ein Wurzelsystem, das dem Gleichungssysteme genügt, so muß in der Matrix, die aus $|\xi_{ij}|$ entsteht, wenn man $x_1, \ldots, x_m$ als $k + 1^{\text{te}}$ Spalte hinzufügt, jede Determinante $k + 1^{\text{ten}}$ Grades

verschwinden. Wenn man die Reihe der Unbekannten x und die Wurzelsysteme ξ_{ij} passend ordnet, kann man voraussetzen, daß die Determinante $|\xi_{ij}|_{(i,j=1,\ldots,k)}$ von 0 verschieden ist, und erhält dann eine Reihe linearer Gleichungen

$$\xi x_{k+l} + \xi_{l1} x_1 + \cdots + \xi_{lk} x_k = 0, \quad (l = 1, \ldots, m-k), \quad \text{(J)}$$

wo ξ eine von 0 verschiedene Größe ist, die den Inhalt des vorgelegten Gleichungssystems vollständig darstellt. Denn infolge der vorausgesetzten Eigenschaft des Systems gibt es ein Wurzelsystem, in dem $x_1, \ldots, x_k$ beliebige Werte annehmen. Ferner muß mit $\xi_{1j}, \ldots, \xi_{mj}$, $(j = 1, \ldots, k)$, weil die Lösungen eben eine Schar bilden, auch

$$x_i = \sum_{j=1}^{k} u_j \xi_{ij} \qquad (i = 1, \ldots, m)$$

ein Wurzelsystem sein, welche Werte immer die Größen u_j annehmen. Aus den Gleichungen

$$x_i = \sum_{j=1}^{k} u_j \xi_{ij} \qquad (i = 1, \ldots, k)$$

ergibt sich aber bei beliebiger Wahl von $x_1, \ldots, x_k$ ein bestimmtes System von Größen u_j, die den Gleichungen genügen. Die zugehörigen $x_{k+1}, \ldots, x_m$ können also keine anderen sein als die durch (J) bestimmten, weil ein solches System jedenfalls existiert und dann auch (J) genügen muß. Wir haben damit folgenden Satz gewonnen:

Wenn der Inhalt eines Gleichungssystems eine k-gliedrige Schar bildet, so wird er vollständig und ausschließlich durch eine lineare Mannigfaltigkeit $m - k^{\text{ter}}$ Stufe dargestellt, welche das Element $(0, 0, \ldots, 0)$ enthält und also durch $m - k$ homogene lineare Gleichungen der Gestalt (J) definiert ist.

Die Umkehrung des Satzes ist evident.

Die diesbezügliche Eigenschaft eines Systems von Gleichungen wird also durch Bildung der Minimalresolvente, d. h. durch eine endliche Reihe rationaler Operationen entschieden; insbesondere bestimmt sich dabei auch die Zahl k.

Die Wichtigkeit des Satzes in den Anwendungen beruht darauf, daß bei gewissen Problemstellungen jene Eigenschaft des Gleichungssystems, daß dessen Inhalt eine Schar bildet, unmittelbar in Evidenz tritt, und man daraus also ohne weiteres schließen darf, daß die linke Seite der Minimalresolvente eine homogene lineare Form von $x, x_{h+1}, \ldots, x_{m-1}$ ist, oder auch, daß der Inhalt jenes Systems durch ein System linearer Gleichungen von der Gestalt (J) definiert wird. Dabei wird nur noch zu berücksichtigen sein, daß die in diesen auftretenden Unbekannten homogene lineare Formen der ursprünglichen Unbekannten $z_1, \ldots, z_m$ sind.

Die Funktionaldeterminante.

§ 14. Sind $F_1, \ldots, F_k$ irgend welche Formen von $x_1, \ldots, x_m$ und $\varphi(z_1, \ldots, z_k)$ eine Form der Unbestimmten $z_1, \ldots, z_k$, so wird

$$\varphi(F_1, F_2, \ldots, F_k)$$

wieder eine Form von $x_1, \ldots, x_m$ darstellen. Die Derivierte dieser Form nach x_j wird durch die Formel

$$\frac{\partial \varphi}{\partial x_j} = \sum_{i=1}^{k} \frac{\partial \varphi}{\partial F_i} \frac{\partial F_i}{\partial x_j} \tag{I}$$

gegeben; diese Regel der Differentialrechnung ist, soweit es sich um Formen (oder ganze Funktionen) handelt, eine einfache Identität, die sich aus der formalen Definition der Derivierten (Kap. II. § 5) direkt ableiten läßt. Setzt man nämlich statt x_j überall $x_j + h_j$, so hat man in φ die Koeffizienten von $h_1, \ldots, h_m$ zu bestimmen, und dazu genügt es, für F überall $F_i + H_i$ und

$$H_i = \sum_{j=1}^{m} \frac{\partial F_i}{\partial x_j} h_j$$

zu setzen, da die wegbleibenden Glieder auf die gesuchten Koeffizienten keinen Einfluß ausüben können. Ebenso wird

$$\varphi(F_1 + H_1, \ldots, F_k + H_k)$$

mit

$$\sum_{i=1}^{k} \frac{\partial \varphi}{\partial F_i} H_i$$

in den Gliedern, die in Bezug auf $h_1, \ldots, h_m$ von der ersten Dimension sind, übereinstimmen, und man erhält also als Koeffizienten von h_j den in (I) stehenden Ausdruck.

Es soll nun insbesondere ein System von m Formen der Unbestimmten $x_1, \ldots .. x_m$

$$F_i(x_1, \ldots, x_m), \quad (i = 1, \ldots, m)$$

betrachtet werden; wir schreiben noch kurz

$$F_{ij} = \frac{\partial F_i}{\partial x_j}$$

und nennen dann

$$|F_{ij}|_{(i,j=1,\ldots,m)}$$

die Funktionaldeterminante*) des Formensystems $F_1, \ldots, F_m$ nach $x_1, \ldots, x_m$.

Für eine Form einer Unbestimmten ist dies nichts anderes als die Derivierte; ist die Anzahl der Unbestimmten größer als 1, so gibt die Funktionaldeterminante eine wichtige Verallgemeinerung dieses Begriffs; sie wird demgemäß auch mit $\frac{\partial(F_1, \ldots, F_m)}{\partial(x_1, \ldots, x_m)}$ oder $\frac{\partial(F)}{\partial(x)}$ bezeichnet.

Sind $\Phi_1, \ldots, \Phi_m$ Formen von $F_1, \ldots, F_m$ und $F_1, \ldots, F_m$ Formen von $x_1, \ldots, x_m$, so kann man $\Phi_1, \ldots, \Phi_m$ auch als Formen von $x_1, \ldots, x_m$ auffassen und hat dann

$$\frac{\partial \Phi_i}{\partial x_j} = \sum_{r=1}^{m} \frac{\partial \Phi_i}{\partial F_r} \frac{\partial F_r}{\partial x_j};$$

---

*) Die fundamentalen Eigenschaften der Funktionaldeterminante wurden zuerst von Jacobi entwickelt. („De determinantibus functionalibus". Journal f. r. u. a. Math., Bd. 22, 1841, pag. 319 = Werke, Bd. III, pag. 393). Eine rein algebraische Theorie wird meines Wissens hier zum ersten Male gegeben.

also nach dem Multiplikationssatze für Determinanten

$$\frac{\partial(\Phi)}{\partial(x)} = \frac{\partial(\Phi)}{\partial(F)} \frac{\partial(F)}{\partial(x)}.$$

Insbesondere kann man auf die Formen F die Transformation

$$x_i = \sum_{j=1}^{m} a_{ij} z_j \quad (i = 1, \ldots, m), \quad |a_{ij}| \neq 0 \qquad \text{(T)}$$

ausüben; sie gehn dadurch in Formen von $z_1, \ldots, z_m$ über, und man hat

$$\frac{\partial F}{\partial z_j} = \sum_{i=1}^{m} \frac{\partial F}{\partial x_i} a_{ij},$$

also

$$\frac{\partial(F)}{\partial(z)} = |a_{ij}| \frac{\partial(F)}{\partial(x)}.$$

Man erhält demnach die Funktionaldeterminante des durch (T) transformierten Systems, wenn man die Funktionaldeterminante des ursprünglichen Systems mit der Determinante der Transformation multipliziert; da diese als von 0 verschieden vorausgesetzt wird, sind beide Funktionaldeterminanten entweder zugleich Null, oder sie sind beide von 0 verschieden.

Die Formen $F_1, \ldots, F_m$ heißen voneinander abhängig, wenn für dieselben eine Identität von der Gestalt

$$\sum_{(g)} C_g F_1^{g_1} \ldots F_m^{g_m} = 0$$

besteht, wo die Größen C_g nicht durchweg verschwinden; im entgegengesetzten Falle heißen sie voneinander unabhängig. Dabei sollen die C_g Größen irgend eines Rationalitätsbereiches sein, in dessen Definition die Unbestimmten $x_1, \ldots, x_m$ nicht eingehn. Man kann aber die Definition der Abhängigkeit, resp. Unabhängigkeit der Formen $F_1, \ldots, F_m$ von vornherein ohne Beschränkung der Allgemeinheit auch so fassen, daß die Größen C dem durch die Koeffizienten der Formen F bestimmten Rationalitätsbereich angehören sollen und nicht sämtlich verschwinden.

Denn wenn irgend welche der ausgesprochenen Bedingung genügende Größen C existieren, genügen sie einem Systeme homogener linearer Gleichungen, in welchem die Koeffizienten jenem durch die Koeffizienten der F bestimmten Rationalitätsbereiche angehören. Man erhält diese Gleichungen durch die Aussage, daß der Koeffizient jedes Potenzproduktes der x gleich 0 sein muß. Dann ist aber jene Identität für jedes Größensystem C gültig, das diesen homogenen linearen Gleichungen genügt. Der Inhalt dieser Gleichungen bildet eine k-gliedrige Schar, wo $k \geqq 1$, da es der Annahme nach eine Lösung gibt, die von $(0, \ldots, 0)$ verschieden ist; und nach der Darstellung der Schar (§ 13) hat man in der Tat auch Größensysteme C, die jenem Rationalitätsbereiche angehören.

Die Abhängigkeit, resp. Unabhängigkeit der Formen $F_1, \ldots, F_m$ steht im engsten Zusammenhange mit ihrer Funktionaldeterminante. Man hat dabei zuerst den folgenden Satz:

Die Funktionaldeterminante eines Systems voneinander abhängiger Formen verschwindet identisch.

Zum Beweise gehn wir von der nun als existierend vorausgesetzten Identität aus, welche die Abhängigkeit der Formen ausdrückt und in der Gestalt

$$\Phi(F_1, \ldots, F_m) = 0$$

geschrieben werden kann. Da dies eben eine Identität ist, hat man auch

$$\frac{\partial \Phi}{\partial x_j} = \sum_{i=1}^{m} \frac{\partial \Phi}{\partial F_i} \frac{\partial F_i}{\partial x_j} = 0, \qquad (j = 1, \ldots, m)$$

also auch:

$$|F_{ij}| \frac{\partial \Phi}{\partial F_j} = 0. \qquad (j = 1, \ldots, m)$$

Es zeigt sich leicht, daß, wenn $|F_{ij}|$ als von 0 verschieden vorausgesetzt wird, im Gegensatze zur Annahme jeder Koeffizient C_g in Φ verschwinden muß. Dann wäre nämlich

$$\frac{\partial \Phi}{\partial F_j} = 0, \qquad (j = 1, \ldots, m)$$

wenn man die linke Seite als Form der x auffaßt, während $\frac{\partial \Phi}{\partial F_j}$ als Form der F nicht für jedes j identisch verschwindet. Sonst wäre ja $\Phi = C$, und C von 0 verschieden, was absurd ist.

War demnach Φ in den F von der n^{ten} Dimension, so führt die Abhängigkeit der Formen bei nicht verschwindender Funktionaldeterminante zu einer Relation

$$\Phi_1(F_1, \ldots, F_m) = 0,$$

wo Φ_1 eine nicht verschwindende Form von der $n-1^{\text{ten}}$ Dimension ist. So weiter schließend gelangt man schließlich zu einer nicht verschwindenden linearen Form Φ_{n-1}, das heißt zu einer Relation

$$C_0 + C_1 F_1 + \cdots + C_m F_m = 0,$$

wo nicht alle C verschwinden. Nach derselben Schlußweise muß nun $\frac{\partial \Phi_{n-1}}{\partial F_j} = C_j$ $(j = 1, \ldots, m)$ hier verschwinden, und da Φ_{n-1} nicht identisch Null ist, einerseits C_0 von 0 verschieden sein, andrerseits die Relation $C_0 = 0$ bestehn. Die Annahme $|F_{ij}| \neq 0$ führt demnach zu einem Widerspruch, womit der ausgesprochene Satz als gültig nachgewiesen ist.

§ 15. Der zuletzt bewiesene Satz läßt sich auch umkehren; er ist demnach als Teilsatz in dem jetzt zu beweisenden allgemeinen Satze enthalten:

(*a*) Die Formen $F_1, \ldots, F_m$ sind dann und nur dann unabhängig, wenn die Funktionaldeterminante $|F_{ij}|$ von 0 verschieden ist.

Dabei soll im vorhinein betont werden, daß wir den Beweis ausschließlich mit der Theorie der algebraischen Größen angehörigen Hilfsmitteln führen und, was für die Anwendung des Satzes unerläßlich ist, zugleich eine Methode entwickeln, welche für den Fall $|F_{ij}| = 0$ mittels rationaler Operationen eine Relation $\Phi(F_1, \ldots, F_m) = 0$ liefert, resp. die Gesamtheit dieser Relationen vollständig charakterisiert.

Der vorzutragende Beweis gestaltet sich durchsichtiger, wenn wir zugleich das System von Gleichungen

$$F_i(x_1, \ldots, x_m) = w_i \quad (i = 1, \ldots, m) \tag{1}$$

betrachten, wo $w_1, \ldots, w_m$ neue Unbestimmte bedeuten, und mit dem obigen Satze zugleich das folgende auf jenes System bezügliche Theorem begründen:

(*b*) Der Inhalt des Systems $F_i = w_i$ bildet eine Mannigfaltigkeit m^{ter} Stufe, wenn $|F_{ij}|$ von 0 verschieden ist; das System $F_i = w_i$ hat keinen Inhalt, wenn $|F_{ij}| = 0$ ist*).

*) Die Bedeutung der w als neuer unbestimmter Größen ist hier genau festzuhalten. Dabei zeigt sich der prinzipielle Unterschied zwischen Unbestimmten und unbeschränkt Veränderlichen in besonders klarer Weise. Für „unbestimmte" w ist der soeben ausgesprochene Satz ausnahmslos gültig. Sind hingegen die w Veränderliche, so ist der Satz, wie man sich auszudrücken pflegt, nur „im allgemeinen" gültig; d. h. er kann seine Gültigkeit nur für eine bestimmte in $(w_1, \ldots, w_m)$ enthaltene Mannigfaltigkeit erster oder höherer Stufe verlieren. Wie sich in diesem Falle die weitere Untersuchung gestaltet, soll hier sogleich kurz angedeutet werden.

Der Satz (*b*) besagt, daß die Gesamtresolvente des Systems $F_i = w_i$ für unbestimmte w im ersten Falle von der Gestalt

$$\Phi(x, t_1, \ldots, t_m, w_1, \ldots, w_m) = 0$$

ist, im zweiten Falle aber Relationen von der Form

$$\Psi(w_1, \ldots, w_m) = \sum_{i=1}^{m} \lambda_i (F_i - w_i)$$

existieren.

Gibt man nun den $w_1, \ldots, w_m$ irgend welche solche Werte, die einer solchen Relation $\Psi = 0$ nicht genügen, so kann das System $F_i - w_i = 0$ keine Lösung besitzen, und damit ist der zweite Fall erledigt.

Im ersten Falle ist die Gesamtresolvente des Systems $F_i = w_i$ für jene speziellen Werte von w zu bilden. Solange nun die Formen $f_{j_{h+1}}^{(h+1)}$ nicht sämtlich verschwinden, geschieht die Bildung der Formen $D_t^{(h)}$ und $f_{j_h}^{(h)}$ genau so, wie für unbestimmte w. Man sieht auch unmittelbar, daß mit den Formen $f_{j_{h+1}}^{(h+1)}$ die Formen der folgenden Systeme $f_{j_{h+2}}^{(h+2)}, \ldots$ gleichfalls identisch verschwinden. Dies geschieht aber auch dann, wenn in den Formen des vorhergehenden Systems, z. B. in $f_{j_k}^{(k)}$

Auch für diesen Satz sei es besonders erwähnt, daß unsre Erörterungen den „Fundamentalsatz der Algebra“ nicht voraussetzen; wir benutzen nur die formentheoretische Definition der algebraischen Größen, und, wie die ausführlichen Erörterungen des Kap. IV gezeigt haben, sind die für diese erhaltenen Resultate nichts anderes als kürzer geschriebene Identitäten für dem ursprünglichen Rationalitätsbereiche entstammende Formen.

Wir bemerken zunächst, daß die Sätze (*a*) und (*b*) für $m = 1$ richtig sind. Ist $m = 1$ (also nur eine Form F_1 und eine Unbestimmte x_1 vorhanden), so kann man wohl den Ausdruck „voneinander unabhängig“ dem gewöhnlichen Sprachgebrauche nach nicht benutzen, aber das Wesen der Sache (wir fragen nach der Existenz einer Form einer Unbestimmten $\varphi(z)$, für welche $\varphi(F_1) = 0$ wird) bleibt davon unberührt. In diesem Falle wird aus der Funktionaldeterminante einfach die Derivierte von F_1, und ihr Verschwinden bedeutet, daß F_1 die Unbestimmte x_1 überhaupt nicht enthält, also $F_1 = A$. Existiert umgekehrt eine Relation $\varphi(F_1) = 0$, so muß F_1 einem Gattungsbereiche angehören, der dem durch die Koeffizienten von φ definierten Rationalitätsbereiche entstammt, also von x_1 unabhängig sein. Da nun aber F_1 eine diesem Rationalitätsbereiche entstammende Form ist, hat man wieder $F_1 = A$. — Ist demnach $\frac{\partial F_1}{\partial x_1}$ von 0 verschieden, so existiert keine Relation $\varphi(F_1) = 0$, und die Gleichung $F_1 = w_1$ gibt eine endliche Anzahl von Wertsystemen für x_1, weil F_1 die Unbekannte x_1 wirklich enthält; ist aber $\frac{\partial F_1}{\partial x_1} = 0$, also $F_1 = A$, so ist dies die behauptete Relation, und die Gleichung $A = w_1$ hat keinen Inhalt.

---

der Koeffizient der höchsten Potenz von x_{k+1} immer gleich Null wird. Sind diese Koeffizienten $G_i^{(k)}(w_1, \ldots, w_m), \ldots$, so bleibt der Satz jedenfalls für alle Wertsysteme $w_1, \ldots, w_m$ gültig, für welche das Produkt $\prod_{(i,k)} G_i^{(k)}$ von 0 verschieden ist.

Um die Sätze (*a*) und (*b*) allgemein zu beweisen, können wir demnach die vollständige Induktion anwenden, d. h. voraussetzen, daß diese für k Formen, resp. Gleichungen mit ebensovielen Unbestimmten, resp. Unbekannten für $k < m$ schon bewiesen sind, und auf dieser Grundlage den Beweis für $k = m$ führen. Dabei sollen wieder die Formen F durch lineare Transformation schon von Zufälligkeiten befreit sein; daß eine solche lineare Transformation an der Gültigkeit der Sätze nichts ändert, ist augenscheinlich.

Die weiteren Ausführungen scheiden sich nun nach dem Range*) der Funktionaldeterminante. Dabei ist zu bemerken, daß, wenn die Funktionaldeterminante den Rang r besitzt, man unbeschadet der Allgemeinheit voraussetzen kann, daß alle Unterdeterminanten

$$|F_{ij}|, \quad (i = 1, \ldots, r; j = j_1, \ldots, j_r),$$

wo $j_1, \ldots, j_r$ aus der Reihe $1, \ldots, m$ gewählte, beliebige r verschiedene Zahlen bedeuten, sämtlich von Null verschieden sind. Daß die in der nicht verschwindenden Unterdeterminante auftretenden Formen gerade $F_1, \ldots, F_r$ sind, verlangt nur die entsprechende Anordnung und Benennung des Formensystems. Wenn nun z. B.

$$|F_{ij}|, \quad (i, j = 1, \ldots, r)$$

nicht verschwindet, wenden wir eine passend gewählte lineare Transformation

$$x_\mu = \sum_{\nu=1}^{m} a_{\mu\nu} z_\nu \qquad (\mu = 1, \ldots, m)$$
$$|a_{\mu\nu}| \neq 0$$

an und betrachten die transformierten Formen. Sollen auch diese von Zufälligkeiten befreit sein, so hat man die $a_{\mu\nu}$ nur so zu wählen, daß sie einer gewissen endlichen Anzahl al-

*) Eine Determinante $|a_{ij}|$, $(i, j = 1, \ldots, m)$ und auch eine Matrix $|a_{ij}|$, $(i = 1, \ldots, p; j = 1, \ldots, q)$ heißt nach Frobenius („Über lineare Gleichungen etc." Journ. f. Math. Bd. 86, pag. 1) vom Range r, wenn r die größte ganze Zahl ist, für welche die Unterdeterminanten r^{ten} Grades nicht sämtlich verschwinden.

gebraischer Gleichungen nicht genügen. Weiter wird, wenn auf der linken Seite F_i die transformierte Form bedeutet:

$$\frac{\partial \overline{F}_i}{\partial z_\nu} = \sum_{\mu=1}^{m} \frac{\partial F_i}{\partial x_\mu} a_{\mu\nu},$$

also für die transformierten Formen irgend eine der in Frage kommenden Unterdeterminanten:

$$|\overline{F}_{i\nu}|_{(i=1,\cdots,r;\,\nu=j_1,\cdots,j_r)} = \left|\sum_{\mu=1}^{m} F_{i\mu}\, a_{\mu\nu}\right|_{(i=1,\cdots,r;\,\nu=j_1,\cdots,j_r)},$$

und diese ist daher nach einem bekannten Determinantensatze*) weiter auch

$$= \sum_{(s)} A_s \Delta_s,$$

wo

$$\Delta_s = |F_{ij}|_{(i=1,\cdots,r;\,j=s_1,\cdots,s_r)},\quad A_s = |a_{ji}|_{(j=s_1,\cdots,s_r;\,i=1,\cdots,r)}$$

und die Summation sich auf alle aus $1, \ldots, m$ möglichen Kombinationen $s_1, \ldots, s_r$ erstreckt. Die bei der Entwicklung der Determinanten A_s auftretenden Potenzprodukte der a sind sämtlich voneinander verschieden; eine Kürzung des Ausdrucks von $\sum_{(s)} A_s \Delta_s$ findet also nicht statt, und es ist demnach

$$|\overline{F}_{i\nu}|_{(i=1,\cdots,r;\,\nu=j_1,\cdots,j_r)}$$

bei jeder Wahl von $j_1, \ldots, j_r$ eine nicht verschwindende Form der a, weil ja der Annahme nach der Koeffizient von

$$|a_{ji}|_{(i,j=1,\cdots,r)},$$

das ist

$$|F_{ij}|_{(i,j=1,\cdots,r)}$$

von 0 verschieden ist.

Man kann also solche Werte der a, auch rationale und ganze Zahlen bestimmen, die auch den Gleichungen $\sum_{(s)} A_s \Delta_s = 0$ nicht genügen, und die Funktionaldeterminante der so transformierten Formen besitzt demnach die behauptete Eigenschaft; es genügt aber, dem Beweise der aufgestellten Sätze das transformierte Formensystem zu Grunde zu legen.

*) S. z. B. Baltzer, Theorie und Anwendung der Determinanten, 4. Aufl., pag. 46.

§ 16. Wir betrachten zuerst den Fall, wo die Funktionaldeterminante vom Range $m-1$ oder m ist, d. h. entweder nicht verschwindet oder, wenn dies der Fall ist, doch eine von Null verschiedene Unterdeterminante $m-1^{\text{ten}}$ Grades besitzt. Nach dem früher Gesagten kann dies dahin präcisiert werden, daß die Unterdeterminanten

$$|F_{ij}|_{(i=1,\cdots,m-1;\ j=j_1,\cdots,j_{m-1})}$$

nach Anwendung einer geeigneten linearen Transformation sämtlich von Null verschieden sind.

Dann sehn wir vor allem, daß der Inhalt des Gleichungssystems

$$F_i = w_i \qquad (i = 1, \ldots, m)$$

keine Mannigfaltigkeit von niedrigerer als m^{ter} Stufe bilden kann. Wäre das der Fall, so hätte das System auch eine Lösung, in der x_{m-1} als Unbestimmte verbleibt; und diese genügt dem Systeme

$$F_i = w_i, \qquad (i = 1, \ldots, m-1)$$

auch dann, wenn wir darin x_{m-1} als Unbestimmte belassen, also nur $x_1, \ldots, x_{m-2}, x_m$ als Unbekannte betrachten. Für dieses System von $m-1$ Gleichungen mit ebensoviel Unbekannten gelten aber unsre Sätze. Diesen Gleichungen genügt also eine endliche Anzahl von Wurzelsystemen, und die darin auftretenden Größen sind bestimmte algebraische Funktionen von $x_{m-1}, w_1, \ldots, w_{m-1}$. Eine der Lösungen müßte aber bei der jetzt untersuchten Annahme auch $F_m = w_m$ genügen, d. h. die neue Unbestimmte w_m wäre eine algebraische Funktion der übrigen, und diese absurde Folgerung zeigt die Unzulässigkeit der Annahme.

Die Gesamtresolvente des Systems $F_i = w_i$ ist also entweder eine Form von $x, t_1, \ldots, t_m, w_1, \ldots, w_m$, wenn das System Lösungen besitzt; oder aber eine Form von $w_1, \ldots, w_m$ allein, wenn es keine Lösungen besitzt.

Wenn wir zunächst den letzteren Fall näher betrachten, hat man nach dem grundlegenden Satze für die Resolventenform (Kap. III. § 18 und § 4 dieses Kapitels):

$$\Phi(w_1, \ldots, w_m) \equiv 0 \quad \left(\text{mod.}\, F_1 - w_1, \ldots, F_m - w_m, x - \sum_{i=1}^{m} x_i t_i\right)$$

oder, dieselbe Tatsache als Identität ausgedrückt,

$$\Phi(w_1, \ldots, w_m) = \sum_{i=1}^{m} \lambda_i (F_i - w_i) + \mu \left(x - \sum_{i=1}^{m} x_i t_i\right).$$

Nach den citierten Stellen hat man eigentlich links immer die Einheit; dann sind aber — wegen der Unbestimmten w, die jetzt in den durch die Koeffizienten des Gleichungssystems definierten Rationalitätsbereich eingehn — in den Formen λ_i und μ die Koeffizienten im allgemeinen Quotienten von Formen der w. Durch Entfernung dieser Nenner erhält man die angeführte Gestalt unsrer Identität, wo nun $\lambda_1, \ldots, \lambda_m$ und μ dem durch die Koeffizienten der Formen F definierten Rationalitätsbereiche entstammende Formen von $x, x_1, \ldots, x_m, t_1, \ldots, t_m, w_1, \ldots, w_m$ sind.

Diese für unbestimmte $x, w_1, \ldots, w_m$ richtige Identität bleibt auch dann richtig, wenn

$$w_i = F_i, \quad x = \sum_{i=1}^{m} x_i t_i$$

gesetzt wird, und ergibt dann

$$\Phi(F_1, \ldots, F_m) = 0,$$

also eine Abhängigkeit der Formen F, und es muß also in diesem Falle die Funktionaldeterminante verschwinden.

Im entgegengesetzten Falle haben wir

$$\Phi(x, w_1, \ldots, w_m) = \sum_{i=1}^{m} \lambda_i (F_i - w_i) + \mu (x - \sum x_i t_i),$$

wo x in Φ wirklich enthalten ist, und zeigen nun, daß dieser Fall mit dem Verschwinden der Funktionaldeterminante nicht verträglich ist. Unter der Voraussetzung einer verschwindenden Funktionaldeterminante setzen wir $x = \sum x_i t_i$ und bezeichnen das Resultat dieser Substitution, wie früher, durch eine eckige Klammer; dann wird

$$[\Phi] = \sum_{i=1}^{m} [\lambda_i] (F_i - w_i)$$

und, wenn man die Derivierte nach x_j bildet:

$$\left[\frac{\partial \Phi}{\partial x}\right] t_j = \sum_{i=1}^{m} \left(\left[\frac{\partial \lambda_i}{\partial x_j}\right] + \left[\frac{\partial \lambda_i}{\partial x}\right] t_j \right) (F_i - w_i) + \sum_{i=1}^{m} [\lambda_i] \frac{\partial F_i}{\partial x_j}$$

$$(j = 1, \ldots, m)$$

und hieraus, wenn man die den Elementen $\frac{\partial F_1}{\partial x_j}$ der Funktionaldeterminante entsprechenden Unterdeterminanten $m - 1^{\text{ten}}$ Grades mit φ_j bezeichnet:

$$\left[\frac{\partial \Phi}{\partial x}\right] \sum_{j=1}^{m} t_j \varphi_j = \sum_{i=1}^{m} A_i (F_i - w_i),$$

wo $\Sigma t_j \varphi_j$ mit φ_m, einer der nicht verschwindenden Unterdeterminanten, von Null verschieden ist. Setzt man in dieser Identität $w_i = F_i$, so muß

$$\left[\frac{\partial \Phi}{\partial x}\right]_{w_i = F_i} = 0$$

sein. Dabei ist $\frac{\partial \Phi}{\partial x} = \Phi_1$ eine Form von $x, t_1, \ldots, t_m, w_1, \ldots, w_m$, die wie Φ in $x, t_1, \ldots, t_m$ homogen, und deren Dimension als Form dieser Unbestimmten um Eins kleiner ist als die von Φ.

Setzt man in Φ_1 zugleich $x = \sum_{i=1}^{m} x_i t_i$, $w_i = F_i$, so verschwindet Φ_1, wie eben bewiesen wurde, eine Tatsache, die wieder durch eine Identität

$$\Phi_1 = \sum_{i=1}^{m} \lambda_i^{(1)} (F_i - w_i) + \mu^{(1)} (x - \Sigma x_i t_i)$$

ausgedrückt werden kann. Dabei ist natürlich Φ_1 mit Φ eine nicht verschwindende Form; der entgegengesetzte Fall könnte nur dann eintreten, wenn Φ die Unbestimmte x nicht enthält, was der jetzt untersuchten Annahme widerspricht. — Auf die so erhaltene Identität lassen sich aber genau dieselben Schlüsse anwenden, wie früher, und man gelangt daher, wenn Φ in x und den t von der s^{ten} Dimension war, schließlich zu einer Identität

$$\Phi_s(w_1, \cdots, w_m) = \sum_{i=1}^{m} \lambda_i^{(s)} (F_i - w_i) + \mu^{(s)} (x - \Sigma x_i t_i),$$

wo Φ_s die Unbestimmten $x, t_1, \ldots, t_m$ nicht mehr enthält und durch die Substitutionen $w_i = F_i$, $x = \Sigma x_i t_i$ unmittelbar die Relation

$$\Phi_s(F_1, \ldots, F_m) = 0$$

ergibt. Dieselbe Identität zeigt aber auch, daß die Annahme einer Gesamtresolvente $\Phi(x, w_1, \ldots, w_m) = 0$ einen Widerspruch enthält; denn dann gäbe es ein Größensystem $\xi_1, \ldots, \xi_m$, das den Gleichungen $F_i = w_i$ genügt. Setzt man dieses für $x, \ldots, x_m$ in der letzten Identität und $x = \Sigma \xi_i t_i$, so wäre $\Phi_s(w_1, \ldots, w_m)$ identisch Null, während doch Φ_s seiner Entstehung nach eine nicht verschwindende Form der w sein soll.

§ 17. Damit sind die zu Beginn des § 15 ausgesprochenen Sätze für den Fall einer Funktionaldeterminante m^{ten} oder $m - 1^{\text{ten}}$ Ranges vollständig bewiesen. Wenn die Funktionaldeterminante vom Range m, d. h. nicht Null ist, also die Formen $F_1, \ldots, F_m$ voneinander unabhängig sind, haben wir nichts weiter hinzuzufügen; im entgegengesetzten Falle ist aber die Abhängigkeit der Formen $F_1, \ldots, F_m$ noch genauer zu präcisieren.

Die Entwicklung der Resolvente, also eine bestimmte Reihe rationaler Operationen, führt dann unbedingt zu einer Relation, die wir wieder

$$\Phi(F_1, \ldots, F_m) = 0$$

schreiben können. Hieraus folgt, wenn man $F_i = w_i + F_i - w_i$ setzt und nach den Potenzprodukten der $F_i - w_i$ entwickelt:

$$\Phi(w_1, \ldots, w_m) = \Sigma \varphi_i(F_i - w_i).$$

Dabei entstammen — ihrer Entstehung nach — die Formen Φ, φ_i dem durch die Koeffizienten der F definierten Rationalitätsbereiche (R).

Sei nun (R) irgend ein Rationalitätsbereich, in dem (R) enthalten ist (insbesondere ein diesem entstammender Gattungsbereich). Dann möge

$$\Phi = \Phi_1 \ldots \Phi_k$$

die Zerlegung von Φ in irreduzible Faktoren in diesem Bereiche darstellen. Setzt man wieder $w_i = F_i$, so wird Φ, also auch einer der Faktoren gleich Null. Es sei dieser Faktor Φ_1. Man hat also schon

$$\Phi_1(F_1, \ldots, F_m) = 0,$$

wo Φ_1 eine in $(\overline{\mathrm{R}})$ irreduzible Form ist.

Ist Ψ irgend eine dem Bereiche $(\overline{\mathrm{R}})$ entstammende Form von $w_1, \ldots, w_m$, so wird dann und nur dann $\Psi(F_1, \ldots, F_m) = 0$, wenn Ψ durch die in diesem Bereiche irreduzible Form Φ_1 teilbar ist.

Daß mit Φ_1 jede durch Φ_1 teilbare Form für $w_i = F_i$ verschwindet, ist unmittelbar einzusehn. Ist Ψ durch Φ_1 nicht teilbar, so wird wegen der Irreduzibilität von Φ_1 auch $(\Psi, \Phi_1) \sim 1$ sein müssen. Eine algebraische Relation zwischen $F_1, \ldots, F_{m-1}$ findet nicht statt, denn wegen

$$|F_{ij}|_{(i,j=1,\cdots,m-1)} \neq 0$$

ist selbst eine Relation

$$\varphi(F_1, \ldots, F_{m-1}, x_m) = 0$$

unmöglich. Φ_1 und Ψ enthalten also w_m. Für die Resultante nach w_m erhält man daher

$$\mathrm{Res.}\begin{pmatrix}\Phi_1, & \Psi\\ w_m, & 1\end{pmatrix} = \psi = W_1\Phi_1 + W_2\Psi,$$

und ψ ist eine nicht verschwindende Form von $w_1, \ldots, w_{m-1}$. Trotzdem müßte, wenn $w_i = F_i, (i = 1, \ldots, m)$ gesetzt wird,

$$\psi(F_1, \ldots, F_{m-1}) = 0$$

sein, und dies ist, wie oben auseinandergesetzt wurde, unmöglich.

Geht man insbesondere (nach Kap. IV. § 18) in jenen Gattungsbereich über, in welchem Φ in absolut irreduzible Faktoren zerfällt, so erhält man eine absolut irreduzible Form $\overline{\Phi}(w_1, \ldots, w_m)$ von der Beschaffenheit, daß die Relation

$$\Psi(F_1, \ldots, F_m) = 0$$

dann und nur dann besteht, wenn $\Psi(w_1, \ldots, w_m)$ durch $\overline{\Phi}(w_1, \ldots, w_m)$ teilbar ist.

§ 18. Wir betrachten nun den Fall, wo die Funktionaldeterminante vom Range $r < m - 1$ ist; wie wir wissen, kann dabei angenommen werden, daß die Determinanten

$$\frac{\partial (F_1, F_2, \ldots, F_r)}{\partial (x_{i_1}, x_{i_2}, \ldots, x_{i_r})}$$

sämtlich von Null verschieden sind. Dagegen wird, wenn $s > r$ und i_s von $i_1, i_2, \ldots, i_r$ verschieden ist, jede Determinante

$$\frac{\partial (F_1, F_2, \ldots, F_r, F_s)}{\partial (x_{i_1}, x_{i_2}, \ldots, x_{i_r}, x_{i_s})}$$

verschwinden. Wir können $F_1, \ldots, F_r, F_s$ als Formen von $x_{i_1}, \ldots, x_{i_r}, x_{i_s}$ auffassen, in denen die Koeffizienten Formen der übrigen $m - r - 1$ Unbestimmten sind, die jetzt mit $z_1, z_2, \ldots, z_{m-r-1}$ bezeichnet werden mögen. Für dieses Formensystem, in dem die Anzahl der Unbestimmten kleiner geworden ist, gelten die im Vorhergehenden bewiesenen Sätze, und da der Rang der Funktionaldeterminante genau gleich der um eine Einheit verringerten Anzahl der Unbestimmten ist, gibt es eine durch rationale Operationen gegebene Form φ, für welche

$$\varphi (F_1, \ldots, F_r, F_s) = 0$$

wird. Allerdings sind die Koeffizienten dieser Form selbst noch Formen der Unbestimmten $z_1, z_2, \ldots$, und jene Identität muß genauer

$$\varphi (z_1, z_2, \ldots, F_1, \ldots, F_r, F_s) = 0$$

geschrieben werden.

Daß eine solche Form φ existiert, welche die Unbestimmten z gar nicht enthält, ist eben nachzuweisen. Aus der letzten Identität hat man jedenfalls auch, wenn $w_i + F_i - w_i$ statt F_i gesetzt wird, durch Entwicklung nach Potenzprodukten der $F_i - w_i$:

$$\varphi (z_1, z_2, \ldots, w_1, \ldots, w_r, w_s) = \sum_{\mu=1, \ldots, r, s} \lambda_\mu (F_\mu - w_\mu).$$

Also auch:

$$\frac{\partial \varphi}{\partial z_1} = \sum \frac{\partial \lambda_\mu}{\partial z_1} (F_\mu - w_\mu) + \sum \lambda_\mu \frac{\partial F_\mu}{\partial z_1},$$

$$0 = \frac{\partial \varphi}{\partial x_i} = \sum \frac{\partial \lambda_\mu}{\partial x_i}(F_\mu - w_\mu) + \sum \lambda_\mu \frac{\partial F_\mu}{\partial x_i},$$
$$i = i_1, \ldots, i_r$$

wo die Summation immer auf $\mu = 1, \ldots, r, s$ bezogen ist, und endlich, wenn man mit den entsprechenden Unterdeterminanten multipliziert und addiert:

$$\frac{\partial (F_1, \ldots, F_r)}{\partial (x_1, \ldots, x_r)} \frac{\partial \varphi}{\partial z_1} = \sum \lambda_\mu^{(1)} (F_\mu - w_\mu).$$

Hier ist links $\frac{\partial (F_1, \ldots, F_r)}{\partial (x_1, \ldots, x_r)}$ von den Unbestimmten w unabhängig und nicht Null; die Form $\frac{\partial \varphi}{\partial z_1}$ gleichfalls nicht Null, weil ja sonst — entgegen der Annahme — φ die Unbestimmte z_1 gar nicht enthalten würde. Setzt man aber $w_\mu = F_\mu$, so muß die linke Seite verschwinden, also $\frac{\partial \varphi}{\partial z_1} = \varphi_1$ eine Form sein, für welche

$$\varphi_1 (z_1, z_2, \ldots, F_1, \ldots, F_r, F_s) = 0.$$

Nun ist φ_1 in z_1 von niedrigerem Grade als φ. Diese Schlußweise führt schließlich zu einer Form

$$\Phi (w_1, \ldots, w_r, w_s),$$

die nicht verschwindet, die Unbestimmten z nicht enthält und für die

$$\Phi (F_1, \ldots, F_r, F_s) = 0$$

wird. Von Φ gehen wir nun ebenso, wie früher, zu der in $(\bar{\mathrm{R}})$ irreduzibeln Form Φ_1, resp. der absolut irreduzibeln Form $\bar{\Phi}$ über. Damit haben wir den folgenden allgemeinen Satz:

Ist die Funktionaldeterminante des Formensystems $F_1, \ldots, F_m$ vom Range r und dementsprechend $\frac{\partial (F_1, \ldots, F_r)}{\partial (x_1, \ldots, x_r)}$ nicht Null, so sind die Formen $F_1, \ldots, F_r$ voneinander unabhängig, während zwischen $F_1, \ldots, F_r, F_s$ $(s > r)$ immer eine algebraische Abhängigkeit besteht. Und zwar gibt es $m - r$ bestimmte, absolut irredu-

zible Formen $\Phi_s(w_1, \ldots, w_r, w_s)$, wo $s = r + 1, \ldots, m$ zu setzen ist, für welche

$$\Phi_s(F_1, \ldots, F_r, F_s) = 0$$

ist. Eine Relation von der Gestalt

$$\Psi_s(F_1, \ldots, F_r, F_s) = 0$$

besteht dann und nur dann, wenn $\Psi_s(w_1, \ldots, w_r, w_s)$ durch $\Phi_s(w_1, \ldots, w_r, w_s)$ teilbar ist.

Daß das Gleichungssystem $F_i = w_i$ $(i = 1, \ldots, m)$, wo $w_1, \ldots, w_m$ neue Unbestimmte bedeuten, niemals einen Inhalt besitzt, wenn der Rang der Funktionaldeterminante kleiner als m ist, folgt aus dem Vorstehenden in einfachster Weise. Denn $\Phi_s(F_1, \ldots, F_r, F_s) = 0$ ergibt wieder

$$\Phi_s(w_1, \ldots, w_r, w_s) = \sum_{\mu=1,\ldots,r,s} \lambda_\mu (F_\mu - w_\mu).$$

Gäbe es nun ein Größensystem, für welches in der Tat $F_\mu(x_1, \ldots, x_m) = w_\mu$, so könnte man dieses rechts einsetzen, und es wäre $\Phi_s(w_1, \ldots, w_r, w_s) = 0$, während doch Φ_s eine von Null verschiedene Form dieser Unbestimmten ist.

Ist das Formensystem

$$F_i(x_1, \ldots, x_m) \qquad (i = 1, \ldots, k)$$

gegeben, so kann nach dem Vorhergehenden immer entschieden werden, ob diese Formen voneinander abhängig sind oder nicht, und in ersterem Falle wird man auch die für sie bestehenden charakteristischen Relationen aufstellen können.

Ist nämlich $k < m$, so ergänze man zu einem Systeme von m Formen mit m Unbestimmten durch Hinzufügung der Null als $k + 1^{\text{ter}}, \ldots, m^{\text{ter}}$ Form.

Ist $k > m$, so betrachte man die Formen als von den Unbestimmten $x_1, \ldots, x_m, x_{m+1}, \ldots, x_k$ abhängig. Da dann $\frac{\partial F_i}{\partial x_{m+1}}, \ldots, \frac{\partial F_i}{\partial x_k}$ verschwinden, ist die Funktionaldeterminante immer Null, und man sieht daraus, daß $m + 1$ oder mehr Formen von m Unbestimmten immer durch algebraische Relationen verknüpft sind.

Sechstes Kapitel.

Resultanten und Discriminanten.

(Spezielle Eliminationstheorie.)

Allgemeine Formen und die diesbezügliche Fragestellung.

§ 1. Als allgemeine Form n^{ter} Dimension der m Unbestimmten $x_1, \ldots, x_m$ bezeichnen wir jene Form, welche alle mit der Dimensionsbestimmung verträglichen Glieder wirklich enthält, während die Koeffizienten der Form durchweg voneinander verschiedene, neue Unbestimmte sind. Wir betrachten sodann das allgemeine Formensystem:

$$F_i(x_1, x_2, \ldots, x_m) = \sum_{(g)} a_g^{(i)} x_1^{g_1^{(i)}} x_2^{g_2^{(i)}} \ldots x_m^{g_m^{(i)}}$$

$$(i = 1, \ldots, k; \quad g_1^{(i)} + \cdots + g_m^{(i)} \leqq n_i)$$

und bezeichnen den Komplex der Unbestimmten, die als Koeffizienten in F_i eingehen, kurz mit $a^{(i)}$ und den Komplex aller $a^{(i)}$ für $i = 1, \ldots, k$ mit a, den Komplex der Unbestimmten $x_1, \ldots, x_m$ endlich, wie dies schon früher geschehen, mit x.

In den speziellen Fällen, wo einzelne unbestimmte Koeffizienten in die Rechnung eingehen, wird es angezeigt sein, für diese einfachere Bezeichnungen zu gebrauchen, die hier sogleich normiert werden sollen. Wir schreiben:

$$F_i(x_1, \ldots, x_m) = \sum_{j=1}^{m} a_{ij} x_j^{n_i} + \cdots + \sum_{j=1}^{m} c_{ij} x_j + a_{i, m+1},$$

d. h. wir bezeichnen den Koeffizienten der ersten und der

höchsten (n_i^{ten}) Potenz von x_j in F_i durch c_{ij}, bez. a_{ij} und das von den Unbestimmten freie Glied dieser Form mit $a_{i,m+1}$.

Die rationalen und ganzen Formen der Unbestimmten a und x bilden nun einen holoiden Bereich, und die in diesem enthaltenen Formen $F_1, \ldots, F_k$ bestimmen, wenn wir sie als „Modulsystem" fassen, einen in jenem Bereiche enthaltenen Kongruenzbereich (Kap. I. § 10),

Ist $E(a, x)$ irgend eine rationale und ganze Form der a und x, so kann durch eine endliche Reihe rationaler Operationen entschieden werden, ob $E(a, x)$ jenem Kongruenzbereich angehört, d. h. in der hierfür eingeführten Bezeichnung, ob

$$E(a, x) \equiv 0 \pmod{F_1, \ldots, F_k}; \tag{1.}$$

und, wenn dies der Fall ist, kann auch eine Darstellung

$$E(a, x) = \sum_{i=1}^{k} H_i F_i, \tag{1.a}$$

wieder durch eine endliche Reihe rationaler Operationen wirklich gefunden werden*).

Die postulierte Fundamentaleigenschaft der Form $E(a, x)$ ist in (1.a) durch eine Identität gegeben, die wir noch in anderer Gestalt schreiben können. Setzt man nämlich**) für $i = 1, \ldots, k$ statt $a_{i,m+1}$ überall $a_{i,m+1} - F_i$, was in diesem Kapitel kurz durch Anwendung einer eckigen Klammer angedeutet werden soll, so wird, wie man unmittelbar sieht,

$$[F_i] = 0, \qquad (i = 1, \ldots, k)$$

und, da die Identität bei dieser Änderung gültig bleibt:

$$[E(a, x)] = 0.$$

Setzt man mit Ausschluß von $a_{1,m+1}$ für jedes $a_{i,m+1}$

*) Die allgemeinste Behandlung dieser „linearen diophantischen Probleme" werden wir in Kap. VII und VIII kennen lernen.

**) Diese wichtige Kroneckersche Substitution wurde schon in Kap. III. § 23 in ihrer einfachsten Gestalt (für eine Form) angewendet.

wieder $a_{i,m+1} - F_i (i = 2, \ldots, k)$, was kurz durch das Zeichen $[\cdots]_1$ angedeutet werden soll, so wird

$$[F_i]_1 = 0, \qquad (i = 2, \ldots, k)$$

und

$$[E(a, x)]_1 = [H_1]_1 F_1,$$

also durch F_1 teilbar.

Die notwendige und hinreichende Bedingung für das Bestehen der Kongruenz

$$E(a, x) \equiv 0 \pmod{F_1, \ldots, F_k}$$

ist:

$$[E(a, x)]_1 \equiv 0 \pmod{F_1}. \tag{2.}$$

Denn diese soeben als notwendig erschlossene Bedingung erweist sich auch als genügend, wenn man bedenkt, daß für jede Form $E(a, x)$ eine Relation

$$E(a, x) \equiv [E(a, x)]_1 + K_2 F_2 + \cdots + K_k F_k$$

besteht, die mit (2.) verbunden, die gesuchte Darstellung unmittelbar ergibt.

Als einfache Anwendung dieser Bezeichnung geben wir sogleich den folgenden vielfach zu gebrauchenden Hilfssatz:

Ist $E(a, x) \equiv 0 \pmod{F_1, \ldots, F_k}$, so enthält die Form E entweder alle Unbestimmten, die als Koeffizienten in F_1 auftreten, wirklich, oder es ist schon $E(a, x) \equiv 0 \pmod{F_2, \ldots, F_k}$.

Ist nämlich $a_g^{(1)}$ irgend ein Koeffizient aus F_1, der in $E(a, x)$ nicht vorkommt, so enthält auch $[E(a, x)]_1$ diesen Koeffizienten nicht; es muß also $[H_1]_1 = 0$ sein, sonst wäre $[E(a, x)]_1 = [H_1]_1 F_1$ eine Form, in welcher $a_g^{(1)}$ zum mindesten mit dem Exponenten 1 wirklich vorkommt. Es ist demnach $[E(a, x)]_1 = 0$, und hieraus folgt in der Tat $E(a, x) \equiv 0 \pmod{F_2, \ldots, F_k}$. Man bemerke noch, daß in diesem Falle die Identität

$$E(a, x) = K_2 F_2 + \cdots + K_k F_k$$

besteht. Ordnet man nun $E(a, x)$ nach den Potenzprodukten

der $a^{(1)}$, so wird für jeden Koeffizienten eines solchen Potenzproduktes $e(a^{(2)}, \ldots, a^{(k)}, x)$ schon

$$e(a^{(2)}, \ldots, a^{(k)}, x) \equiv 0 \pmod{F_2, \ldots, F_k}$$

sein, wie die Vergleichung der Koeffizienten auf beiden Seiten unmittelbar ergibt, wenn man bedenkt, daß die Formen $F_2, \ldots, F_k$ die Unbestimmten $a^{(1)}$ nicht enthalten.

§ 2. Wir spezialisieren das vorgelegte Problem weiter, indem wir uns auf rationale und ganze Formen $\Theta(a)$ der Unbestimmten a, welche die x gar nicht enthalten, beschränken; auf diese ist das allgemeine Problem leicht zurückzuführen, wie später (§ 6) gezeigt werden soll.

Für solche Formen $\Theta(a)$ erhalten wir nun zuerst den wichtigen Satz:

Sind $F_1, \ldots, F_k$ wirkliche Formen der x, d. h. ihre Dimension zumindest gleich Eins und ist

$$\Theta(a) \equiv 0 \pmod{F_1, \ldots, F_k},$$

während $k \leqq m$, so folgt hieraus $\Theta(a) = 0$, d. h. ist die Anzahl der allgemeinen Formen im System nicht größer als die Anzahl der Unbestimmten x, so ist die Null die einzige rationale und ganze Form der Unbestimmten a, welche jener Kongruenz genügt.

Für den Beweis genügt es, den Fall $k = m$ zu betrachten. Denn wenn $k < m$, kann man das System durch weitere allgemeine Formen $F_{k+1}, \ldots, F_m$ ergänzen. Nach dieser Ergänzung ist mit $\Theta(a) \equiv 0 \pmod{F_1, \ldots, F_k}$ auch $\Theta(a) \equiv 0 \pmod{F_1, \ldots, F_m}$, und der Satz ist allgemein bewiesen, wenn wir aus dieser Kongruenz $\Theta(a) = 0$ folgern.

Diese Folgerung ergibt sich unmittelbar aus dem Satze (b) des § 15 im vorhergehenden Kapitel. Die Funktionaldeterminante des allgemeinen Formensystems $F_1, \ldots, F_m$ ist nicht Null; denn sie wird z. B. von Null verschieden, wenn $F_i = x_i^{m_i}$ gesetzt wird. Das von $x_1, \ldots, x_m$ freie Glied in F_i ist eine Unbestimmte $a_{i,m+1}$. Der Inhalt des Gleichungssystems

$F_i = 0$ bildet also eine Mannigfaltigkeit m^{ter} Stufe, d. h. das System hat eine Lösung, die aus gewissen algebraischen Funktionen der a besteht. Setzt man diese in $F_1, \ldots, F_m$ ein, so wird aus der Identität

$$\Theta(a) = \sum_{i=1}^{m} H_i F_i,$$

da jedes F_i verschwindet, während sich Θ, das die x gar nicht enthält, überhaupt nicht ändert, dem Satze entsprechend $\Theta(a) = 0$.

Vom didaktischen Standpunkte aus kann es bequem sein, die Darstellung dieses Kapitels von der allgemeinen Theorie der Elimination unabhängig zu gestalten. Es möge daher noch ein zweiter Beweis des Satzes folgen, obwohl kein prinzipieller Unterschied obwaltet, da, wie schon seinerzeit betont wurde, auch dort von dem s. g. Fundamentalsatze der Algebra kein Gebrauch gemacht wurde.

Wir benutzen jetzt die vollständige Induktion. Für $m = 1$ ist der Satz unmittelbar klar. $\Theta(a) \equiv 0 \pmod{F_1}$ wäre ein Ausdruck für die Tatsache, daß $\Theta(a)$ durch F_1 teilbar ist, was, da $\Theta(a)$ die x nicht enthält, nicht möglich ist, wenn $\Theta(a)$ von Null verschieden ist.

Wir setzen nun den Satz für Formen mit m Unbestimmten als richtig voraus und gehen in folgender Weise auf Formen mit $m + 1$ Unbestimmten über.

Ist $\Theta(a) \equiv 0 \pmod{F_1, F_2, \ldots, F_{m+1}}$, so enthält (nach dem Hilfssatz in § 1) $\Theta(a)$ entweder die Unbestimmte a_{11} oder es ist auch $\Theta(a) \equiv 0 \pmod{F_2, \ldots, F_{m+1}}$. Im letzteren Falle muß $\Theta(a)$ entweder a_{22} enthalten oder aber schon $\Theta(a) \equiv 0 \pmod{F_3, \ldots, F_{m+1}}$ gelten. Würde immer der zweite Fall auftreten, so hätte man schließlich $\Theta(a) \equiv 0 \pmod{F_{m+1}}$; da dies unmöglich ist, muß also $\Theta(a)$ eine Unbestimmte a_{ii} enthalten, und man kann — unbeschadet der Allgemeinheit — voraussetzen, daß diese Unbestimmte a_{11} ist; hierzu ist nur eine passende Anordnung der Unbestimmten x und der Formen F notwendig.

Ordnet man $\Theta(a)$ nach Potenzen von a_{11}, so wird

$$\Theta(a) = \Theta_0 + \Theta_1 a_{11} + \cdots + \Theta_r a_{11}^r;$$

und es ist $r \geqq 1$, $\Theta_r \not\equiv 0$. Aus der Identität

$$\Theta(a) = \sum_{i=1}^{m+1} H_i F_i = H_1 (a_{11} x_1^{n_1} + \cdots) + \sum_{i=2}^{m+1} H_i F_i$$

ergibt sich aber, wenn man den Koeffizienten der höchsten Potenz von a_{11} auf beiden Seiten vergleicht,

$$\Theta_r = G_1 x_1 + G_2 F_2 + \cdots + G_{m+1} F_{m+1},$$

wo G_1, falls H_1 in Bezug auf a_{11} von niedrigerem als dem $r - 1^{\text{ten}}$ Grade ist, gleich Null zu setzen wäre. Setzt man hier $x_1 = 0$, so wird

$$\Theta_r = [G_2]_{x_1=0} \cdot [F_2]_{x_1=0} + \cdots + [G_{m+1}]_{x_1=0} \cdot [F_{m+1}]_{x_1=0} \cdot$$

Setzt man aber in allgemeinen Formen von $m+1$ Unbestimmten für x_1 Null, so werden aus diesen allgemeine Formen von m Unbestimmten, und, da für diese der Satz richtig ist, müßte die als von Null verschieden vorausgesetzte Form Θ_r Null sein. Die Annahme $\Theta(a) \equiv 0$ (mod. $F_1, \ldots, F_{m+1}$) führt also zu einem Widerspruche, sobald $\Theta(a)$ nicht Null ist.

Definition und fundamentale Eigenschaften der Resultante.

§ 3. Für das System von $m+1$ allgemeinen Formen der m Unbestimmten

$$F_i(x_1, \ldots, x_m), \qquad (i = 1, \ldots, m+1),$$

deren Dimensionen $n_1, \ldots, n_{m+1}$ durchweg $\geqq 1$ seien, gilt der fundamentale Satz:

Es gibt eine und nur eine — im Sinne der Äquivalenz vollständig bestimmte — rationale und ganze irreduzible Form der unbestimmten Koeffizienten a, die dem durch das Modulsystem $(F_1, \ldots, F_{m+1})$ be-

stimmten Kongruenzbereich angehört. Sie wird die Resultante jenes Formensystems genannt und mit

$$R = \text{Res. } (F_1, F_2, \ldots, F_{m+1})$$

bezeichnet.

Setzt man an Stelle der unbestimmten Koeffizienten a irgend welche einem holoiden Bereiche (A) angehörige Größen, die nur der Bedingung unterworfen sind, daß die so entstehenden Formen wieder von der Dimension $n_1, \ldots, n_{m+1}$ seien, so nennt man die aus der Resultante sich ergebende Größe wieder die Resultante jener speziellen Form und bezeichnet sie mit

$$\text{Res.} \begin{pmatrix} F_1, F_2, \ldots, F_m, F_{m+1} \\ x_1, x_2, \ldots, x_m, 1 \end{pmatrix}.$$

Diese ausführlichere Bezeichnung ist deshalb notwendig, weil jetzt auch andere Unbestimmte in den Formen enthalten sein können.

Es wird sich zeigen, daß die Definition der Resultante zweier Formen mit einer Unbestimmten, deren Theorie in Kap. III behandelt wurde, in diesen Betrachtungen als spezieller Fall enthalten ist.

Das Vorzeichen der Resultante ist ihrer Definition nach vorläufig unbestimmt; seine Bestimmung bleibt vorbehalten.

Der Satz ergibt sich unmittelbar aus der allgemeinen Theorie der Elimination. Der Inhalt des Systems von Gleichungen $F_1 = 0, \ldots, F_m = 0$ bildet — wie schon früher erwähnt — eine Mannigfaltigkeit m^{ter} Stufe; die so bestimmten (in endlicher Anzahl vorhandenen) Wurzelsysteme können der Gleichung $F_{m+1} = 0$ niemals genügen, da die Koeffizienten dieser Gleichung durchaus neue Unbestimmte sind. Das System $F_1 = 0, \ldots, F_{m+1} = 0$ hat demnach keinen Inhalt, und die Theorie der Resolventenform führt unmittelbar zu einer rationalen und ganzen Form $\Phi(a)$, für welche

$$\Phi(a) \equiv 0 \pmod{F_1, \ldots, F_{m+1}}.$$

Gibt es aber überhaupt eine von Null verschie-

dene rationale und ganze Form der Koeffizienten a, die dem durch das Modulsystem $(F_1, \ldots, F_{m+1})$ definierten Kongruenzbereich angehört, so gilt der zu Beginn ausgesprochene Satz, und jede solche Form ist durch R teilbar.

Man zerlege nämlich $\Phi(a)$ in seine irreduzibeln Faktoren

$$\Phi(a) = P_1(a) \ldots P_r(a).$$

Setzt man dann wieder $a_{i,m+1} - F_i$ für $a_{i,m+1}$, so wird

$$[\Phi(a)] = [P_1(a)] \ldots [P_r(a)] = 0;$$

also einer der Faktoren rechts z. B. $[P(a)] = 0$; d. h. es ist auch

$$P(a) \equiv 0 \pmod{F_1, \ldots, F_{m+1}}.$$

Es kann aber dann für eine zweite, mit $P(a)$ nicht äquivalente irreduzible rationale und ganze Form $Q(a)$ niemals

$$Q(a) \equiv 0 \pmod{F_1, \ldots, F_{m+1}}$$

sein. $P(a)$ und $Q(a)$ sind beide von Null verschieden und enthalten alle Koeffizienten $a_g^{(i)}$; wenn auch nur ein solcher ausfällt, müßte $P(a)$, resp. $Q(a)$ nach § 1 schon dem durch $(F_1, \ldots, F_{m+1})$ mit Ausschluß von F_i definierten Kongruenzbereiche angehören und also nach dem Satz in § 2 gleich Null sein.

Bildet man nun die Resultante von $P(a)$ und $Q(a)$ in Bezug auf $a_g^{(i)}$ — nach der in Kap. III entwickelten elementaren Theorie — so wird

$$\begin{aligned}\text{Res.} \begin{pmatrix} P(a), & Q(a) \\ a_g^{(i)}, & 1 \end{pmatrix} &= Q_1(a)\, P(a) + P_1(a)\, Q(a) \\ &\equiv 0 \pmod{F_1, \ldots, F_{m+1}}\end{aligned}$$

und, da dies eine rationale und ganze Form der Koeffizienten a mit Ausschluß von $a_g^{(i)}$ ist, muß diese Resultante gleich Null sein; es hätten also die nicht äquivalenten irreduzibeln Formen $P(a)$ und $Q(a)$ — im Gegensatze zu dieser Annahme — einen gemeinsamen Teiler, der von Eins verschieden. Damit ist aber

der Satz erwiesen. Ist nämlich irgend ein $\Psi(a) \equiv 0$ (mod. $F_1, \ldots, F_{m+1}$), so muß für einen irreduzibeln Teiler dieser Form, $Q(a)$, schon $Q(a) \equiv 0$ und $P(a) \sim Q(a)$, also $\Psi(a)$ durch $P(a)$ teilbar sein.

Wir entwickeln jetzt die allgemeine Theorie der Resultanten ohne Benutzung der allgemeinen Theorie der Elimination, nicht bloß aus didaktischen Gründen, sondern vor allem, weil wir dabei zugleich die rekursive Bildung der Resultante eines Formensystems in möglichst einfacher Weise bewerkstelligen.

§ 4. Die Methode, deren wir uns bedienen, ist die der vollständigen Induktion, und es wird dementsprechend zuerst der Fall $m = 1$ zu erledigen sein. Dabei haben wir nur die früher Kap. III. § 14 erhaltenen Resultate zu ergänzen. Indem wir nur die Bezeichnungen den jetzigen allgemeinen Festsetzungen gemäß ändern, sind die beiden Formen

$$F_1(x_1) = a_{11} x_1^{n_1} + \cdots + a_{12}$$
$$F_2(x_1) = a_{21} x_1^{n_2} + \cdots + a_{22},$$

und die dort aufgestellte Sylvestersche Determinante ist auch in dem jetzt gegebenen genaueren Sinne die Resultante des Formensystems F_1, F_2. Um diese Behauptung zu erweisen, haben wir nur zu zeigen, daß sie eine irreduzible Form der Koeffizienten ist; daß sie dem durch das Modulsystem (F_1, F_2) definierten Kongruenzbereiche angehört, ist schon in Kap. III. § 16 gezeigt worden.

Die fragliche Determinante hat — wie ihr Anblick unmittelbar zeigt — die Entwicklung

$$a_{11}^{n_2} a_{22}^{n_1} + \cdots,$$

wo die ausgeschriebenen Glieder gegen keine andern gekürzt werden können.

Der Kernpunkt des Beweises liegt in der Tatsache, daß, wenn $\Theta(a)$ von Null verschieden und

$$\Theta(a) \equiv 0 \pmod{F_1, F_2}$$

ist, in der Entwicklung von $\Theta(a)$ nach Potenzen von a_{11}:

$$\Theta(a) = \vartheta_0 + \vartheta_1 a_{11} + \cdots + \vartheta_r a_{11}^r$$

ϑ_r durch $a_{22}^{n_1}$ teilbar sein muß*).

Man hat

$$\Theta(a) = H_1 F_1 + H_2 F_2;$$

also, wenn man $a_{22} - F_2$ für a_{22} setzt

$$[\Theta(a)]_1 = [H_1]_1 F_1$$

oder

$$[\vartheta_0]_1 + \cdots + [\vartheta_r]_1 a_{11}^r = [H_1]_1 F_1,$$

also, wenn man die Koeffizienten von a_{11}^r auf beiden Seiten vergleicht,

$$[\vartheta_r]_1 = K x_1^{n_1}$$

oder

$$\vartheta_r = K x_1^{n_1} + L F_2,$$

wo ϑ_r nicht Null sein kann, da $\Theta(a)$ von Null verschieden ist. Ferner muß $r \geqq 1$ sein, da $\Theta(a)$ nach dem Früheren jedenfalls a_{11} enthält. Setzt man in der zuletzt erhaltenen Identität $x_1 = 0$, so wird

$$\vartheta_r = (L)_{x_1=0} \cdot a_{22},$$

also jedenfalls durch a_{22} teilbar.

Wäre nun ϑ_r durch $a_{22}^{n_1-k}$ $(k > 0)$ teilbar, aber durch $a_{22}^{n_1-k+1}$ nicht teilbar, demnach

$$\vartheta_r = a_{22}^{n_1-k} \eta_r,$$

wo η_r wieder eine rationale und ganze Form der a ist, so würde hieraus

$$[a_{22}^{n_1-k}]_1 \cdot [\eta_r]_1 = K x_1^{n_1}$$

oder

$$(a_{22} - F_2)^{n_1-k} \cdot [\eta_r]_1 = K x_1^{n_1}$$

---

*) Dieser Satz, sowie der entsprechende allgemeinere Satz in § 9 ist von F. Mertens gegeben worden. („Über die bestimmenden Eigenschaften der Resultante", Sitzungsber. d. k. Akad. d. Wiss. in Wien. Math. naturwiss. Cl., XCIII. Bd., II. Abt., pag. 548.)

folgen. Es ist aber $(a_{22} - F_2)^{n_1-k}$ durch $x_1^{n_1-k}$ und durch keine höhere Potenz von x_1 teilbar; also wäre

$$[\eta_r]_1 = Mx_1^k,$$
$$\eta_r = Mx_1^k + NF_2;$$

und, wenn man schließlich wieder $x_1 = 0$ setzt,

$$\eta_r = (N)_{x_1=0} \cdot a_{22},$$

d. h. η_r durch a_{22}, und ϑ_r im Widerspruch zur Annahme durch $a_{22}^{n_1-k+1}$ teilbar.

Hätte nun die Sylvestersche Determinante Teiler, so müßte jedenfalls einer davon a_{11} enthalten, und dieser würde, nach Potenzen von a_{11} geordnet, ein höchstes Glied von der Gestalt

$$a_{11}^r a_{22}^{n_1} A$$

besitzen. Da aber die Sylvestersche Determinante augenscheinlich eine homogene Form n_1^{ter} Dimension der Unbestimmten $a^{(2)}$ ist, also auch ihre Teiler nicht von höherer Dimension in den $a^{(2)}$ sein können, muß, wenn man die Rollen der Formen F_1 und F_2 vertauscht, in demjenigen Teiler, der ein Glied mit $a_{22}^{n_1}$ enthält, dieses Glied auch durch $a_{11}^{n_2}$ teilbar sein, d. h. der supponierte Teiler hätte die Gestalt

$$a_{11}^{n_2} a_{22}^{n_1} A + \cdots;$$

dann muß aber $A = 1$ sein, und jener Teiler stimmt vollständig mit der Sylvesterschen Determinante überein, was eben zu beweisen war.

§ 5. Für das System von $m + 1$ allgemeinen Formen mit m Unbestimmten

$$F_i(x_1, \ldots, x_m) \qquad (i = 1, \ldots, m + 1)$$

formulieren wir die zu beweisenden Tatsachen in folgender Weise. Es seien $n_1, \ldots, n_{m+1}$ die Dimension von $F_1, \ldots, F_{m+1}$ und

$$N = n_1 \ldots n_{m+1}, \quad N_i = \frac{N}{n_i}.$$

Dann gibt es eine und nur eine rationale und ganze Form der sämtlichen Koeffizienten a, die s. g. Resultante*) des Formensystems $R(a)$, die folgende Eigenschaften besitzt:

a) Die Resultante ist eine irreduzible Form der a.

b) Es ist $R(a) \equiv 0 \pmod{F_1, \ldots, F_{m+1}}$.

Diese beiden Eigenschaften bestimmen die Resultante bis auf das Vorzeichen.

c) Die Resultante enthält das Glied

$$a_{11}^{N_1} a_{22}^{N_2} \ldots a_{m+1,m+1}^{N_{m+1}}$$

mit dem Koeffizienten $+1$.

Damit ist auch das Vorzeichen der Resultante festgelegt.

d) Die Resultante ist eine homogene Form N_i^{ter} Dimension jeder Koeffizientenreihe $a^{(i)}$; also eine homogene Form von der Dimension $\sum_{i=1}^{m+1} N_i$ der sämtlichen Koeffizienten a.

e) Die Resultante ist isobarisch, d. h. jedes Glied der Resultante ist vom gleichen Gewicht N. Dabei ist unter dem Gewichte des Koeffizienten $a_g^{(i)}$ die Zahl $n_i - \sum_{j=1}^{m} g_j$ und unter dem Gewichte eines Gliedes die Summe der Ge-

---

*) In Bezug auf die Geschichte und die ziemlich ausgedehnte Literatur der Theorie der Resultante soll auf die Encyklopädie der mathematischen Wissenschaften, Bd. I. Abschnitt „Rationale Funktionen mehrerer Veränderlichen" von E. Netto, Art. 6—8 und 14 verwiesen werden.

Eine klare Einsicht in die Natur dieser komplizierten Bildung wird erst durch die Theorie der algebraischen Größen vermittelt. Dabei sind insbesondere die in § 3 gegebene erste Definition der Resultante und die prinzipielle Anwendung der Kroneckerschen Substitution zu betonen. Vielfache Berührungspunkte mit der hier gegebenen Darstellung bieten die beiden Arbeiten von F. Mertens in den Sitz.-Ber. d. Wiener Akad. d. Wiss. XCIII. Bd. II. Abt., pag. 527 (1886) und CVIII. Bd. II. Abt., pag. 1173 (1899); in diesen wird die Kroneckersche Substitution zum ersten Male für das Resultantenproblem verwertet.

wichte der einzelnen in ihm als Faktoren enthaltenen $a_g^{(i)}$ zu verstehen. Bezeichnet man das Gewicht von $a_g^{(i)}$ mit $P(a_g^{(i)})$, so ist demnach

$$P(a_g^{(i')} a_g^{(i'')} \ldots) = P(a_g^{(i')}) + P(a_g^{(i'')}) + \cdots$$

Wir zeigen zuerst, daß aus den Eigenschaften (a), (b), (c) der Resultante immer auch schon (d) und (e) folgen.

Wäre nämlich $R(a)$ in Bezug auf irgend eine Koeffizientenreihe $a_g^{(i)}$ nicht homogen, sondern

$$R(a) = S_{i0} + \cdots + S_{ir},$$

wo S_{ik} den Komplex derjenigen Glieder von $R(a)$ bedeutet, die in Bezug auf die $a_g^{(i)}$ von der k^{ten} Dimension sind, so müßte wegen

$$R(a) = \sum_{i=1}^{m+1} H_i F_i$$

auch*)

$$S_{ir} = H_{ii}^{(r-1)} F_i + \sum_{j=1}^{m} {}^{(i)} H_{ji}^{(r)} F_j$$

sein, wo $H_{ji}^{(s)}$ den Komplex jener Glieder aus H_j bedeutet, die in Bezug auf die Koeffizientenreihe $a_g^{(i)}$ von der s^{ten} Dimension sind. Dann wird aber nach den in § 3 bewiesenen Sätzen die Resultante mit einem irreduzibeln Faktor von S_{ir} übereinstimmen. $R(a) - S_{ir}$ ist also durch $R(a)$ teilbar; da aber $R(a) - S_{ir}$ in den $a_g^{(i)}$ höchstens von der $r - 1^{\text{ten}}$ Dimension, $R(a)$ aber von der r^{ten} Dimension ist, muß also $R(a) - S_{ir} = 0$, d. h. $S_{ir} = R(a)$ sein.

Aus der Existenz der Resultante folgt demnach schon, daß diese eine homogene Form jeder Koeffizientenreihe $a_g^{(i)}$, also auch sämtlicher Koeffizienten a ist.

Wegen (c) ist die Dimension von $R(a)$ in Bezug auf

---

*) Das Zeichen $\sum_{j=1}^{m+1} {}^{(i)}$ bedeutet die Summation über $j = 1, \ldots, m+1$ mit Ausschluß von $j = i$.

die Koeffizientenreihe $a_g^{(i)}$ jedenfalls N_i. Es folgt also in der Tat aus (a), (b) und (c) immer auch (d).

Um dasselbe für (e) zu erschließen, setze man

$$R(a) = T_0(a) + \cdots + T_p(a) + \cdots + T_r(a), \qquad (T_r(a) \neq 0)$$

wo $T_p(a)$ den Komplex derjenigen Glieder von $R(a)$ bedeutet, die vom Gewichte p sind. Die Identität

$$R(a) = \sum_{i=1}^{m+1} H_i F_i$$

wird auch dann richtig bleiben, wenn man überall

$$a_g^{(i)} x_{m+1}^{n_i - \Sigma g_j^{(i)}} \text{ an die Stelle von } a_g^{(i)}$$

setzt. Es ist aber dann

$$\sum_{p=0}^{r} T_p(a) x_{m+1}^p = \sum_{i=1}^{m+1} K_i \Phi_i,$$

da in $T_p(a)$ die Glieder von gleichem Gewichte sind, also sich nur mit x_{m+1}^p multiplizieren, während rechts durch diese Änderung aus F_i die entsprechende homogene Form Φ_i (Kap. II. § 8) entsteht.

Setzt man weiter für $j = 1, \ldots, m+1$ immer $x_j u$ an die Stelle von x_j, so tritt zu Φ_i nur der Faktor u^{n_i} hinzu, und wenn man nun wieder $x_{m+1} = 1$ setzt, wird

$$\sum_{p=0}^{r} T_p(a) u^p = \sum_{i=1}^{m+1} L_i F_i$$

oder, wenn man den Koeffizienten von u^r auf beiden Seiten vergleicht:

$$T_r(a) = \sum_{i=1}^{m+1} M_i F_i.$$

Es muß demnach $T_r(a)$ durch $R(a)$ teilbar sein, also wird auch:

$$R(a) - T_r(a) = T_0(a) + \cdots + T_{r-1}(a) = R(a) Q(a).$$

Dies ist aber unmöglich; denn auf der einen Seite hat man wenigstens ein Glied, dessen Gewicht $\geqq r$, auf der anderen

Seite nur Glieder, deren Gewicht $< r$ ist. Der Widerspruch löst sich nur dann, wenn $R(a) = T_r(a)$ ist. Hiernach hat jedes Glied der Resultante das Gewicht r, und es ist auch $R(a) = T_r(a)$.

Da nun $P(a_{11}) = 0, \ldots, P(a_{nn}) = 0$, $P(a_{m+1,m+1}) = n_{m+1}$, so ist das Gewicht des durch (c) bestimmten Gliedes der Resultante $n_{m+1} N_{m+1} = N$.

Für die Resultante zweier Formen mit einer Unbestimmten gelten diese Behauptungen durchweg. Es ist (a) und (b) im vorhergehenden bewiesen, (c) und (d) sind durch die ausgeschriebene Gestalt der Resultante (Sylvestersche Determinante) unmittelbar evident, und aus diesen folgt, wie eben gezeigt wurde, auch (e).

§ 6. Aus den Sätzen des § 5 ziehen wir noch weitere wichtige Folgerungen. Unter Berücksichtigung der durch

$$F_i(x_1, \ldots, x_m) = \sum_{j=1}^{m} a_{ij} x_j^{n_i} + \cdots + \sum_{j=1}^{m} c_{ij} x_j + a_{i,m+1}$$

festgelegten Bedeutung der Koeffizienten c_{ij} und $a_{i,m+1}$ erhält man aus der Identität

$$R(a) = \sum_{i=1}^{m+1} H_i F_i,$$

wenn man nach c_{ij} und nach $a_{i,m+1}$ deriviert,

$$\frac{\partial R}{\partial c_{ij}} = \sum_{i=1}^{m+1} \frac{\partial H_i}{\partial c_{ij}} F_i + H_i x_j$$

$$\frac{\partial R}{\partial a_{i,m+1}} = \sum_{i=1}^{m+1} \frac{\partial H_i}{\partial a_{i,m+1}} F_i + H_i,$$

also schließlich

$$\frac{\partial R}{\partial a_{i,m+1}} x_j \equiv \frac{\partial R}{\partial c_{ij}} \quad (\text{mod. } F_1, \ldots, F_{m+1}). \qquad (X_j)$$

$$(j = 1, \ldots, m)$$

Ist nun $E(x, a)$ irgend eine rationale und ganze Form

der x und a und als Form der Unbestimmten von der Dimension ν, so wird

$$\left(\frac{\partial R}{\partial a_{i,m+1}}\right)^{\nu} E(x, a)$$

unmittelbar so geschrieben werden können, daß jedes x_j immer nur in dem Produkte $\frac{\partial R}{\partial a_{i,m+1}} x_j$ erscheint; bei Benutzung der Kongruenzen (X_j) erhält man demnach

$$\left(\frac{\partial R}{\partial a_{i,m+1}}\right)^{\nu} E(x, a) \equiv e(a) \pmod{F_1, \ldots, F_{m+1}},$$

wo $e(a)$ eine rationale und ganze Form der a allein ist.

Die notwendige und hinreichende Bedingung für $E(x, a) \equiv 0 \pmod{F_1, \ldots, F_{m+1}}$ ist dann $e(a) \equiv 0 \pmod{F_1, \ldots, F_{m+1}}$ oder also $e(a) \equiv 0 \pmod{R}$.

Daß aus $E(x, a) \equiv 0$ unmittelbar $e(a) \equiv 0$ folgt, ist aus der letzten Kongruenz ersichtlich; aber auch umgekehrt folgt aus dieser Kongruenz, wenn $e(a) \equiv 0$ ist, indem überall $a_{i,m+1} - F_i$ für $a_{i,m+1}$ gesetzt wird,

$$\left[\frac{\partial R}{\partial a_{i,m+1}}\right]^{\nu} [E(x, a)] = 0.$$

Nun kann nicht

$$\left[\frac{\partial R}{\partial a_{i,m+1}}\right] = 0, \text{ d. h. } \frac{\partial R}{\partial a_{i,m+1}} \equiv 0 \pmod{F_1, \ldots, F_{m+1}}$$

sein, weil die Form $\frac{\partial R}{\partial a_{i,m+1}}$ von der Dimension $\Sigma N_i - 1$ nicht durch die Form R von der Dimension ΣN_i teilbar sein kann. Es ist also

$$[E(x, a)] = 0, \text{ d. h. } E(x, a) \equiv 0 \pmod{F_1, \ldots, F_{m+1}}.$$

Rekursive Bildung der Resultante.

§ 7. Wir wollen jetzt die Richtigkeit der Resultantensätze für $m + 1$ Formen mit m Unbestimmten als erwiesen voraussetzen, wie dies für $m = 1$ tatsächlich der Fall ist, und zeigen, daß diese Sätze dann auch für $m + 2$ Formen mit

$m+1$ Unbestimmten ihre Geltung behalten. Dem Wesen der Sache nach geschieht dies, indem wir eine rekursive Methode zur Bildung der Resultante angeben.

Aus einem System von $m+2$ Formen mit m Unbestimmten

$$F_i(x_1, \ldots, x_m) = \sum a_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$
$$(i = 1, \ldots, m+2)$$

entsteht das zu betrachtende System von $m+2$ Formen mit $m+1$ Unbestimmten

$$\overline{F}_i(x_1, \ldots, x_m, x_{m+1}) = \sum \bar{a}_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$
$$(i = 1, \ldots, m+2)$$

— wie unmittelbar ersichtlich — wenn man unter $\bar{a}_g^{(i)}$ eine allgemeine Form der neuen Unbestimmten x_{m+1} vom Grade $n_i - \Sigma g_j$ (dem Gewichte von $a_g^{(i)}$) versteht. Wendet man insbesondere die Schreibart

$$F_i(x_1, \ldots, x_m) = \sum_{j=1}^{m} a_{ij} x_j^{n_i} + \cdots + \sum_{j=1}^{m} c_{ij} x_j + a_{i,m+1}$$

an, so wird

$$\overline{F}_i(x_1, \ldots, x_m, x_{m+1}) = \sum_{j=1}^{m} a_{ij} x_j^{n_i} + \cdots + \sum_{j=1}^{m} \bar{c}_{ij} x_j + \bar{a}_{i,m+1}$$

geschrieben werden können, da $\bar{a}_{ij}$ vom Grade 0 in x_{m+1} ist und daher $\bar{a}_{ij}$ genau denselben Koeffizienten wie a_{ij} bedeutet. Im allgemeinen beschreiben wir:

$$\bar{a}_{ii} = k_{ii} = l_{ii} \qquad (i = 1, \ldots, m)$$
$$\bar{a}_{i,m+1} = k_{i,m+1} + \cdots + l_{i,m+1} x_{m+1}^{n_i}$$
$$\bar{a}_g^{(i)} = k_g^{(i)} + \cdots + l_g^{(i)} x_{m+1}^{n_i - \Sigma g_j}.$$

Eine spezielle Bezeichnung der zwischenliegenden Koeffizienten wird sich als überflüssig erweisen.

Betrachtet man das System S_{m+2} der Formen $\overline{F}_i$ mit Ausschluß einer, z. B. der letzten F_{m+2}, so kann man diese als Formen von $x_1, \ldots, x_m$ mit den Koeffizienten $\bar{a}_g^{(i)}$ ansehen

und erhält nach der für solche erwiesenen fundamentalen Eigenschaft der Resultante die Identität

$$R_{m+2}(\bar{a}) = \sum_{i=1}^{m+1} H_i F_i,$$

oder also auch

$$R_{m+2}(\bar{a}) \equiv 0 \pmod{\bar{F}_1, \ldots, \bar{F}_{m+1}, \bar{F}_{m+2}}. \qquad \text{(I)}$$

Dabei ist $R_{m+2}(\bar{a})$ eine Form der Unbestimmten x_{m+1}, und man erhält deren von x_{m+1} freies Glied, wenn man $x_{m+1} = 0$ setzt oder, was auf dasselbe hinausläuft, wenn man statt $\bar{a}_g^{(i)}$ überall $k_g^{(i)}$ setzt. Dieses kann also mit $R_{m+2}(k)$ bezeichnet werden und ist nichts anderes als die Resultante der $m+1$ allgemeinen Formen mit m Unbestimmten

$$K_i(x_1, \ldots, x_m) = \Sigma k_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$
$$(i = 1, \ldots, m+1).$$

Es ist weiter $R_{m+2}(\bar{a})$ vom Gewichte $\bar{N}_{m+2}$, wenn $\bar{N} = \prod_{i=1}^{m+2} n_i$ und $\bar{N}_p = \frac{\bar{N}}{n_p}$ gesetzt wird. Da nun der Grad von $\bar{a}_g^{(i)}$ in x_{m+1} genau mit dem Gewichte von $a_g^{(i)}$ übereinstimmt, ist jedes Glied von $R_{m+2}(\bar{a})$ vom Grade $\bar{N}_{m+2}$ in x_{m+1}, und man erhält den Koeffizienten der höchsten Potenz von x_{m+1}, wenn man statt $\bar{a}_g^{(i)}$ überall $l_g^{(i)} x_{m+1}^{n_i - \Sigma g_j}$ setzt. Es wird demnach

$$R_{m+2}(\bar{a}) = R_{m+2}(k) + \cdots + R_{m+2}(l)\, x_{m+1}^{\bar{N}_{m+2}},$$

wo wieder $R_{m+2}(l)$ die Resultante der $m+1$ allgemeinen Formen mit m Unbestimmten

$$L_i(x_1, \ldots, x_m) = \Sigma l_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$
$$(i = 1, \ldots, m+1)$$

ist.

Nach (c) in § 5 wird weiter

$$R_{m+2}(k) = k_{11}^{\bar{N}_{m+2,1}} k_{22}^{\bar{N}_{m+2,2}} \ldots k_{m+1,m+1}^{\bar{N}_{m+2,m+1}} + \ldots,$$

wo

$$\bar{N}_{pi} = \frac{\bar{N}_p}{n_i}$$

ist. Genau ebenso wird

$$R_{m+2}(l) = l_{11}^{\overline{N}_{m+2,1}} l_{22}^{\overline{N}_{m+2,2}} \dots l_{m+1,m+1}^{\overline{N}_{m+2,m+1}} + \dots$$

Nun ist nach (c) in § 5 das hinzugeschriebene Glied in $R_{m+2}(k)$ und $R_{m+2}(l)$ das einzige, das nur $k_{11}, k_{22}, \dots, k_{mm}$ und $k_{m+1,m+1}$, resp. $l_{11}, l_{22}, \dots, l_{mm}, l_{m+1,m+1}$ enthält. Da ferner in $R_{m+2}(\bar{a})$ jedes Glied mit Ausnahme von

$$\bar{a}_{11}^{\overline{N}_{m+2,1}} \bar{a}_{22}^{\overline{N}_{m+2,2}} \bar{a}_{m+1,m+1}^{\overline{N}_{m+2,m+1}}$$

wenigstens eine Unbestimmte $\bar{a}_{ij}\,(i \neq j)$ enthält, wird in der Entwicklung von

$$R_{m+2}(\bar{a}) = \left(k_{11}^{\overline{N}_{m+2,1}} \dots k_{m+1,m+1}^{\overline{N}_{m+2,m+1}} + \dots\right) + \dots +$$
$$+ \left(l_{11}^{\overline{N}_{m+2,1}} \dots l_{mm}^{\overline{N}_{m+2,m}} l_{m+1,m+1}^{\overline{N}_{m+2,m+1}} + \dots\right) x_{m+1}^{\overline{N}_{m+2}}$$

jedes Glied — außer den beiden wirklich hingeschriebenen — zumindest einen von $k_{11}, \dots, k_{m+1,m+1}$ und $l_{11}, \dots, l_{m+1,m+1}$ verschiedenen Koeffizienten der Formen $\overline{F}_i$ enthalten.

Wir wollen endlich bei den Formen $\overline{F}_i$ eine Bezeichnung einführen, die von der ursprünglich angewandten Gestalt der Formen F_i unabhängig ist, und gebrauchen dabei, um Unklarheiten zu vermeiden, für die unbestimmten Koeffizienten ein neues Symbol α, d. h. es sei jetzt

$$\overline{F}_i(x_1, \dots, x_{m+1}) = \sum_{j=1}^{m+1} \alpha_{ij} x_j^n + \dots + \alpha_{i,m+2};$$

dann hat man endlich als Schlußresultat, wenn $R_{m+2}(\bar{a})$ als Form der α und x_{m+1} jetzt $R_{m+2}(\alpha, x_{m+1})$ geschrieben wird:

$$R_{m+2}(\alpha, x_{m+1}) = \left(\alpha_{11}^{\overline{N}_{m+2,1}} \dots \alpha_{mm}^{\overline{N}_{m+2,m}} \alpha_{m+1,m+2}^{\overline{N}_{m+2,m+1}} + \dots\right) + \dots +$$
$$+ \left(\alpha_{11}^{\overline{N}_{m+2,1}} \dots \alpha_{mm}^{\overline{N}_{m+2,m}} \alpha_{m+1,m+1}^{\overline{N}_{m+2,m+1}} + \dots\right) x_{m+1}^{\overline{N}_{m+2}} \qquad \text{(I)}$$
$$R_{m+2}(\alpha, x_{m+1}) \equiv 0 \pmod{\overline{F}_1, \dots, \overline{F}_{m+2}}.$$

Dabei sei nochmals bemerkt, daß jedes nicht hingeschriebene Glied von R_{m+2} zumindest eine von

$$\alpha_{11}, \dots, \alpha_{m+2,m+2}, \alpha_{m+1,m+2}, \alpha_{m+2,m+1}$$

verschiedene Unbestimmte enthält; dies ist für die aufgezählten Unbestimmten mit Ausnahme von $\alpha_{m+2,m+1}$ und $\alpha_{m+2,m+2}$ schon früher erwähnt worden. Diese beiden können weiter hinzugefügt werden, da bei der Bildung von R_{m+2} die Form $\overline{F}_{m+2}$ gar nicht benutzt wird.

Bei der Bildung von R_{m+2} wurde aus dem System $\overline{F}_i$ die Form $\overline{F}_{m+2}$ ausgeschlossen; genau dieselbe Entwicklung kann für das Formensystem $\overline{F}_i$ mit Ausschluß von $\overline{F}_{m+1}$ vorgenommen werden, und das Resultat wird sich von dem früheren nur insofern unterscheiden, als die Indices $m+1$ und $m+2$, wenn sie sich auf Formen beziehen, miteinander zu vertauschen sind. Dies hat demnach in den Indices von n, R und $\overline{N}$, ferner in dem ersten Index von α_{ij} und endlich im oberen Index von $\alpha_g^{(i)}$ zu geschehen. In dieser Weise erhält man:

$$\begin{aligned} R_{m+1}(\alpha, x_{m+1}) &= \left(\alpha_{11}^{\overline{N}_{m+1,1}} \dots \alpha_{mm}^{\overline{N}_{m+1,m}} \alpha_{m+2,m+2}^{\overline{N}_{m+1,m+2}} + \dots\right) + \dots + \\ &+ \left(\alpha_{11}^{\overline{N}_{m+1,1}} \dots \alpha_{mm}^{\overline{N}_{m+1,m}} \alpha_{m+2,m+1}^{\overline{N}_{m+1,m+2}} + \dots\right) x_{m+1}^{\overline{N}_{m+1}} \\ R_{m+1}(\alpha, x_{m+1}) &\equiv 0 \pmod{\overline{F}_1, \dots, \overline{F}_{m+2}}, \end{aligned} \tag{II}$$

und jedes nicht ausgeschriebene Glied in R_{m+1} enthält wieder eine von

$$\alpha_{11}, \dots, \alpha_{m+2,m+2}, \quad \alpha_{m+1,m+2}, \quad \alpha_{m+2,m+1}$$

verschiedene Unbestimmte.

Bildet man nun die Resultante von R_{m+1} und R_{m+2} in Bezug auf x_{m+1}, so wird

$$\text{Res.} \begin{pmatrix} R_{m+1}, & R_{m+2} \\ x_{m+1}, & 1 \end{pmatrix} = \alpha_{11}^{K_1} \dots \alpha_{m+2,m+2}^{K_{m+2}} + \dots = H(\alpha), \tag{III}$$

wo jedes weitere Glied, wie aus den bisherigen Erörterungen unmittelbar folgt, zumindest eine von $\alpha_{11}, \dots, \alpha_{m+2,m+2}$ verschiedene Unbestimmte enthält, also jenes erste Glied gegen kein anderes gekürzt werden kann. Das entsprechende Potenzprodukt muß also in $H(\alpha)$ mit dem Koeffizienten Eins auf-

treten. Nun ist für $H(\alpha)$ nach der elementaren Theorie der Resultante von zwei Formen mit einer Unbestimmten

$$H(\alpha) \equiv 0 \pmod{R_{m+1},\ R_{m+2}},$$

also auch

$$H(\alpha) \equiv 0 \pmod{\overline{F}_1, \ldots, \overline{F}_{m+2}}.$$

Damit ist aber nach § 3 die Existenz der Resultante für das allgemeine System von $m+2$ Formen mit $m+1$ Unbestimmten erwiesen, und diese ist als irreduzibler Teiler von $H(\alpha)$ bis auf das Vorzeichen bestimmt. Die Behauptungen (a) und (b) des allgemeinen Satzes in § 5 sind somit erledigt.

§ 8. Die hierin enthaltene Anweisung zur Bildung der Resultante ist noch insofern unvollkommen, als sie eine an dem irreduzibeln Teiler von $H(\alpha)$ anzustellende Versuchsreihe erfordert. An ihre Stelle kann aber eine Methode gesetzt werden, die nur die Bildung von Resultanten für $k+1$ Formen mit k Unbestimmten ($k \leqq m$) und die Bestimmung größter gemeinschaftlicher Teiler verlangt. Diese Methode ergibt zugleich weitere Eigenschaften der Resultanten.

Wendet man die Formeln (X_j) des § 6 auf das Formensystem

$$\overline{F}_i(x_1, \ldots, x_{m+1}) + \sum_{(g)} \bar{a}_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$
$$(i = 1, \ldots m+1)$$

und dessen Resultante $R_{m+2}(\bar{a})$ an, so werden diese:

$$\frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,m+1}} x_j \equiv \frac{\partial R_{m+2}(\bar{a})}{\partial \bar{c}_{ij}} \pmod{\overline{F}_1 \ldots \overline{F}_{m+1}},$$

und ergeben, wie dort, wenn für $E(x, a)$

$$\overline{F}_{m+2}(x_1 \ldots x_{m+1}) = \sum_{(g)} \bar{a}_g^{(m+2)} x_1^{g_1} \ldots x_m^{g_m}$$

gesetzt wird:

$$\left(\frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,m+1}}\right)^{n_{m+2}} \overline{F}_{m+2}(x_1 \ldots x_{m+1})$$
$$\equiv \Gamma(\alpha, x_{m+1}) \pmod{\overline{F}_1, \ldots, \overline{F}_{m+1}}.$$

Dabei ist Γ eine lineare Form der in $\overline{F}_{m+2}$ auftretenden unbestimmten Koeffizienten, da R_{m+2} und dessen Derivierte von diesen frei sind. Davon ausgehend, kann man zeigen, daß der größte gemeinschaftliche Teiler von R_{m+2} und Γ die Eins ist. Nennen wir ihn D, so kann er als Teiler von R_{m+2} keine Unbestimmte $\alpha_g^{(m+2)}$ enthalten. Es muß also, wenn wir Γ als lineare Form der Unbestimmten schreiben, jeder Koeffizient, also auch der von $\alpha_{m+2,m+2}$, d. i.

$$\left(\frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,m+1}}\right)^{n_{m+2}}$$

durch D teilbar sein. Es müßten daher

$$R_{m+2}(\bar{a}) \quad \text{und} \quad \frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,m+1}}$$

einen von 1 verschiedenen Teiler haben. Dieser hätte jedenfalls die Gestalt

$$A_0 + A_1 x_{m+1} + \cdots,$$

wo A_0 nicht 0 ist, weil R_{m+2} nicht durch x_{m+1} teilbar ist. Es muß demnach auch

$$[R_{m+2}(\bar{a})]_{x_{m+1}=0} \quad \text{und} \quad \left[\frac{\partial R_{m+2}(\bar{a})}{\partial \bar{a}_{i,m+1}}\right]_{x_{m+1}=0}$$

durch A_0 teilbar sein. Nun ist die erste Form nichts anderes als die Resultante des allgemeinen Formensystems $[\overline{F}_i]_{x_{m+1}=0}$ $(i = 1, \ldots, m+1)$, also irreduzibel, und die zweite in den $a_g^{(i)}$ von niedrigerem Grade als die erste, folglich muß $A_0 = \pm 1$ sein.

Weiter ist $R_{m+2}(\bar{a})$ homogen in den Unbestimmten $\alpha_g^{(i)}$; jeder Teiler von $R_{m+2}(\bar{a})$ besitzt demnach dieselbe Eigenschaft; es müssen also auch $A_1, \ldots$ rationale und ganze Zahlen sein. Der supponierte Teiler muß demnach eine rationale und ganze Form der einen Unbestimmten x_{m+1} sein. Einen solchen Teiler, der nicht ~ 1 ist, kann aber R_{m+2} nicht besitzen, denn derselbe Teiler müßte in $R_{m+2}(\bar{a})$ enthalten sein, wenn man

$$\bar{a}_g^{(i)} = a_g^{(i)}$$

setzt, indem man dies jetzt nicht durch die Substitution $x_{m+1} = 0$, sondern dadurch erreicht, daß man die in $\bar{a}_g^{(i)}$ als Koeffizienten von $x_{m+1}, x_{m+1}^2, \ldots$ auftretenden Unbestimmten gleich Null setzt. Dann müßte jener Teiler also in

$$[R_{m+2}(\bar{a})]_{x_{m+1}=0}$$

enthalten sein, kann daher x_{m+1} überhaupt nicht enthalten, womit die Tatsache $(R_{m+2}, \Gamma) \sim 1$ erwiesen ist.

Bildet man nun

$$\Delta_{m+2} = \text{Res.}\begin{pmatrix} R_{m+2}(\alpha, x_{m+1}), & \Gamma(\alpha, x_{m+1}) \\ x_{m+1} & , \quad 1 \end{pmatrix},$$

so ist Δ_{m+2} jedenfalls von 0 verschieden, in der Koeffizientenreihe $\alpha_g^{(m+2)}$ vom Grade $\bar{N}_{m+2}$, und man hat auch

$$\Delta_{m+2} \equiv 0 \ (\text{mod. } \bar{F}_1, \ldots, \bar{F}_{m+2}).$$

Indem man der Reihe nach den Formen $\bar{F}_1, \ldots, \bar{F}_{m+1}$ jene Sonderstellung anweist, die in der durchgeführten Entwicklung der Form $\bar{F}_{m+2}$ zukommt, erhält man eine Reihe rationaler und ganzer Formen

$$\Delta_i(\alpha) \qquad (i = 1, \ldots, m+2)$$

von der Beschaffenheit, daß $\Delta_i(\alpha)$ in den $\alpha_g^{(i)}$ von der Dimension $\bar{N}_i$ ist, und für jede dieser Formen

$$\Delta_i(\alpha) \equiv 0 \ (\text{mod. } \bar{F}_1, \ldots, \bar{F}_{m+2})$$

wird. Die Resultante des Formensystems F_i ist also jedenfalls ein gemeinsamer Teiler der Formen Δ_i.

§ 9. Wir unterbrechen den bisherigen Gedankengang, um den folgenden wichtigen Hilfssatz*) zu beweisen.

Ist $\Theta(a)$ nicht Null und

$$\Theta(a) \equiv 0 \ (\text{mod. } F_1, \ldots, F_{m+1}),$$

*) F. Mertens, a. a. O.

so ist in der Entwicklung von Θ nach Potenzen von a_{kk}:

$$\Theta(a) = \vartheta_0 + \cdots + \vartheta_r a_{kk}^r$$

ϑ_r durch $R_{0k}^{n_k}$ teilbar, wo R_{0k} die Resultante des (allgemeinen) Formensystems

$$(F_1)_{x_k=0}, \ldots, (F_{m+1})_{x_k=0}$$

mit Ausschluß von $(F_k)_{x_k=0}$ bedeutet.

Man hat

$$\Theta(a) = \sum_{i=1}^{m+1} H_i F_i,$$

also, wenn man für $i = 1, \ldots, m+1$ mit Ausschluß von $i = k$ immer $a_{i,m+1} - F_i$ für $a_{i,m+1}$ setzt und diese Substitution mit $[\cdots]_k$ bezeichnet,

$$[\vartheta_o]_k + \cdots + [\vartheta_r]_k \alpha_{kk}^r = [H_k]_k F_k$$

oder, wenn man die Koeffizienten α_{kk}^r auf beiden Seiten vergleicht:

$$[\vartheta_r]_k = K x_k^{n_k}$$

und

$$\vartheta_r = K x_k^{n_k} + \sum_{i=1}^{m+1}{}^{(k)} L_i F_i,$$

wo ϑ_r nicht Null ist, da Θ von Null verschieden. Setzt man in der zuletzt erhaltenen Identität $x_k = 0$, so wird

$$\vartheta_r = \sum_{i=1}^{m+1}{}^{(k)} (L_i)_{x_k=0} (F_i)_{x_k=0},$$

also ist jedenfalls ϑ_r durch R_{0k} teilbar.

Wäre nun ϑ_r durch $R_{0k}^{n_k - l}$ teilbar, $(l > 0)$, aber durch $R_{0k}^{n_k - l + 1}$ nicht teilbar, demnach

$$\vartheta_r = R_{0k}^{n_k - l} \eta_r,$$

wo η_r wieder eine rationale und ganze Form der a ist, so würde hieraus

$$[R_{0k}]_k^{n_k-l}[\eta_r]_k = K x_k^{n_k}$$

folgen. Nun ist

$$R_{0k} = \sum_{i=1}^{m+1}{}^{(k)} \lambda_i (F_i)_{x_k=0},$$

wo (nach § 2) λ_i nicht Null ist und R_{0h} die Unbestimmten c_{ik} (den unbestimmten Koeffizienten von x_k in F_i) nicht enthält, da dieser schon aus $(F_i)_{x_k=0}$ entfällt. Man kann daher auch

$$R_{0k} = \sum_{i=1}^{m+1}{}^{(k)} \lambda_i \big((F_i)_{x_k=0} - F_i\big) + \sum_{i=1}^{m+1}{}^{(k)} \lambda_i F_i$$

schreiben und hat demnach

$$[R_{0k}]_k = \sum_{i=1}^{m+1}{}^{(k)} [\lambda_i]_k \big((F_i)_{x_k=0} - F_i\big).$$

Es ist demnach mit $(F_i)_{x_k=0} - F_i$ auch $[R_{0k}]_k$ durch x_k teilbar, dagegegen kann $[R_{0k}]_k$ durch x_k^2 nicht teilbar sein; denn hieraus ergäbe sich, daß, wenn $j \neq k$ ist, auch

$$\frac{\partial}{\partial c_{jk}}[R_{0k}]_k = \left[\frac{\partial R_{0k}}{\partial a_{j,m+1}}\right]_k \frac{\partial (a_{j,m+1} - F_j)}{\partial c_{jk}} = -\left[\frac{\partial R_{0k}}{\partial a_{j,m+1}}\right]_k x_k$$

durch x_k^2, also $\left[\dfrac{\partial R_{0k}}{\partial a_{j,m+1}}\right]_k$ durch x_k teilbar ist. Demnach hätte man eine Relation

$$\frac{\partial R_{0k}}{\partial a_{j,m+1}} = K_k' x_k + \sum_{i=1}^{m+1}{}^{(k)} K_i' F_i$$

oder schließlich, indem man $x_k = 0$ setzt:

$$\frac{\partial R_{0k}}{\partial a_{j,m+1}} \equiv 0 \pmod{(F_1)_{x_k=0}, \ldots, (F_{m+1})_{x_k=0}},$$

wo das Modulsystem $(F_k)_{x_k=0}$ nicht enthält, d. h. $\dfrac{\partial R_{0k}}{\partial a_{j,m+1}}$ wäre durch R_{0k} teilbar, was nicht möglich ist.

Da demnach $[R_{0k}]_k$ genau durch die erste Potenz von x_k teilbar ist, muß $[R_{0k}]_k^{n_k-l}$ genau durch $x_k^{n_k-l}$ teilbar sein, und es wäre $[\eta_r]_k$ durch x_k', also η_r durch R_{0k} teilbar, ϑ_r im Widerspruche zur Annahme nicht bloß durch $R_{0k}^{n_k-l}$, sondern auch

durch $R_{0k}^{n_k-l+1}$ teilbar. Da dieser Schluß, solange $l > 0$, wiederholt werden kann, erhält man den zu Beginn ausgesprochenen Satz.

Hieraus erschließt man aber unmittelbar, daß, wenn das Formensystem $F_1, \ldots, F_{m+1}$ überhaupt eine Resultante besitzt, diese als Form der Koeffizienten $a_g^{(i)}$ nicht von niedrigerer als der N_i^{ten} Dimension sein kann.

Sie enthält die Glieder $a_{kk}^r R_{0k}^{n_k} A$, wo A eine von Null verschiedene Form der a. Nun ist, da die Resultantensätze für m allgemeine Formen mit $m-1$ Unbestimmten als bewiesen vorausgesetzt werden, $R_{0k}^{n_k}$ in den $a_g^{(i)}$ in der Tat von der Dimension N_i.

§ 10. Auf Grundlage dieser Hilfssätze haben wir das folgende Bildungsgesetz der Resultante:

Die Resultante des allgemeinen Formensystems $\bar{F}_i(x_1, \ldots, x_{m+1})$ $(i = 1, \ldots, m+2)$ ist der größte gemeinschaftliche Teiler der Formen

$$H, \Delta_i (i = 1, \ldots, m+2).$$

Mit Ausnahme des elementaren schon früher erledigten Falles $m = 0$ erfordert die Bildung der Formen Δ nur die Darstellung der Resultanten für $k+1$ allgemeine Formen mit k Unbestimmten, wo $k < m+1$ ist.

Die Fundamentaloperationen, aus denen sich schließlich jede Resultantenbildung zusammensetzt, sind demnach die Aufstellung Sylvesterscher Determinanten und die Bestimmung des größten gemeinschaftlichen Teilers von rationalen und ganzen Formen.

Die Resultante, deren Existenz schon in § 7 bewiesen wurde, ist jedenfalls ein gemeinsamer Teiler der Formen Δ_i. Da Δ_i in den Koeffizienten von $\bar{F}_i$ vom Grade $\bar{N}_i$ ist, kann die Resultante R selbst auch nicht von höherem Grade sein. Da sie, wie eben bewiesen wurde, auch nicht von niedrigerem Grade sein kann, wird, wenn

$$\Delta_i = \Delta_i' R$$

gesetzt wird, A_i' diese Koeffizienten nicht mehr enthalten. Der größte gemeinschaftliche Teiler von $A_1', A_2', \ldots$ kann daher nur eine rationale, ganze Zahl k sein. Es ist demnach

$$(A_1, \ldots, A_{m+2}) \sim kR.$$

Ferner ist die unter (III) in § 7 definierte Form H jedenfalls primitiv, mithin hat man

$$R \sim (H, A_1, \ldots, A_{m+2})$$

und damit ist die Resultante bis auf das Vorzeichen bestimmt.

Da die Resultante jedenfalls ein Teiler von

$$H(\alpha) = \alpha_{11}^{K_1} \alpha_{22}^{K_2} \cdots \alpha_{m+2,m+2}^{K_{m+2}} + \cdots$$

ist, muß sie Glieder mit Potenzprodukten von der Gestalt

$$\alpha_{11}^{k_1} \alpha_{22}^{k_2} \cdots \alpha_{m+2,m+2}^{k_{m+2}}$$

enthalten; ferner ist diese Resultante eine homogene Form N_i^{ter} Dimension der $\alpha_g^{(i)}$, es muß also $k_i = \bar{N}_i$ sein, d. h. sie besitzt nur ein Glied der angegebenen Gestalt, und dieses ist

$$\pm \alpha_{11}^{\bar{N}_1} \alpha_{22}^{\bar{N}_2} \cdots \alpha_{m+2,m+2}^{\bar{N}_{m+2}};$$

wäre nämlich der Koeffizient k und nicht ± 1, so würde auch das ausgeschriebene Glied in $H(\alpha)$ den Koeffizienten k enthalten.

Indem man für jenes Glied das obere Vorzeichen wählt, ist die Resultante vollständig bestimmt. Sie besitzt neben (*a*) und (*b*) auch die zu Beginn des § 5 mit (*c*) bezeichnete Eigenschaft, aus denen endlich, wie dort erörtert wurde, auch (*d*) und (*e*) folgen.

Das Vorzeichen der Resultante ist dadurch bestimmt, daß man das Vorzeichen des „Hauptgliedes“ $a_{11}^{N_1} \ldots a_{m+1,m+1}^{N_{m+1}}$ als positiv fixiert. (Wir beziehen uns jetzt, da die vollständige Induktion die Richtigkeit der Resultantensätze gezeigt hat, wieder auf das Formensystem $F_i(x_1, \cdots, x_m)\,(i = 1, \cdots, m+1)$). Schreibt man aber die Formen in irgend einer Reihenfolge $F_{i_1}, \ldots, F_{i_{m+1}}$ und ändert auch die Reihenfolge der Unbestimmten so, daß $x_{j_1}, \ldots, x_{j_m}$ aufeinander folgen, so wird das Hauptglied

$$a_{i_1 j_1}^{N_{i_1}} a_{i_2 j_2}^{N_{i_2}} \dots a_{i_m j_m}^{N_{i_m}} a_{i_{m+1}, j_{m+1}}^{N_{i_{m+1}}},$$

und das Vorzeichen dieses Gliedes ist nun positiv zu nehmen. Bezeichnet man diese Resultante mit R_{ij}, so ist jedenfalls

$$R_{ij} \equiv 0 \pmod{F_1, \dots, F_{m+1}},$$

also R_{ij} durch R und ebenso R durch R_{ij} teilbar. Die Reihenfolge der Formen F und der Unbestimmten x kann folglich nur das Vorzeichen ändern. Um das Gesetz zu bestimmen, nach welchem diese Änderung des Vorzeichens geschieht, werden wir irgend welche spezielle Werte der $a_g^{(i)}$ wählen können, wenn nur für diese die Resultante nicht Null wird.

Vertauscht man zuerst

$$F_i = a_{ii} x_i^{n_i} + \dots + a_{ij} x_j^{n_i} + \dots$$

mit

$$F_j = a_{ji} x_i^{n_j} + \dots + a_{jj} x_j^{n_j} + \dots$$

und dann auch x_i mit x_j, so geht a_{ii} in a_{jj} und a_{jj} in a_{ii} über; die übrigen Größen des Hauptgliedes und dieses selbst bleiben ungeändert. Die Vertauschung von x_i und x_j gibt daher dann und nur dann eine Änderung des Vorzeichens, wenn dies bei der Vertauschung von F_i und F_j der Fall ist.

Wir beweisen leicht das folgende Gesetz:

Die Vertauschung zweier Formen F_i und F_j (und auch zweier Unbestimmten x_i und x_j) ändert das Vorzeichen der Resultante dann und nur dann, wenn alle Formen des Systems ungerader Dimension sind.

In Zeichen ausgedrückt

$$\text{Res.}\begin{pmatrix} \dots, F_i, \dots, F_j, \dots \\ x_1, x_2, \dots, x_m, 1 \end{pmatrix} = (-1)^N \text{Res.}\begin{pmatrix} \dots, F_j, \dots, F_i, \dots \\ x_1, x_2, \dots, x_m, 1 \end{pmatrix}$$

und

$$\text{Res.}\begin{pmatrix} F_1, F_2, \dots, F_{m+1} \\ \dots, x_i, \dots, x_j, \dots, 1 \end{pmatrix} = (-1)^N \text{Res.}\begin{pmatrix} F_1, F_2, \dots, F_{m+1} \\ \dots, x_j, \dots, x_i, \dots, 1 \end{pmatrix}.$$

Die Richtigkeit des Satzes für $m = 1$ erhellt aus dem Anblick der Sylvesterschen Determinante. Diese ist

$$a_{11}^{n_2} a_{22}^{n_1} + \dots + (-1)^{n_1 n_2} a_{21}^{n_1} a_{12}^{n_2}$$

und wird, wenn man die Rolle der beiden Formen vertauscht:

$$a_{21}^{n_1} a_{12}^{n_2} + \cdots + (-1)^{n_1 n_2} a_{11}^{n_1} a_{22}^{n_2},$$

es tritt also dem Satze entsprechend der Faktor $(-1)^{n_1 n_2}$ hinzu.

Um im allgemeinen die aus der Vertauschung von F_i und F_j sich ergebende Änderung der Resultante zu bestimmen, spezialisieren wir irgend eine dritte Form F_k in folgender Weise:

$$F_k = a_{kk} x_k^{n_k}.$$

Die Resultante von $F_1, \ldots, F_{m+1}$ wird dann

$$a_{kk}^{N_k} R_{0k}^{n_k},$$

wo R_{0k} die Resultante von $(F_1)_{x_k=0}, \ldots, (F_{m+1})_{x_k=0}$ mit Ausschluß von $(F_k)_{x_k=0}$ ist. Denn diese Resultante ist eine homogene Form N_k^{ter} Dimension der $a_g^{(k)}$, es kann also bei der angegebenen Spezialisation nur der mit $a_{kk}^{N_k}$ multiplizierte Teil zurückbleiben, und dieser hat nach § 9 und 10 die angegebene Gestalt.

Setzt man das zu beweisende Gesetz für Systeme von weniger als $m+1$ Formen als bewiesen voraus, so wird der Schluß von m auf $m+1$ wieder dessen allgemeine Gültigkeit ergeben, da es für zwei Formen richtig ist. Die Vertauschung von F_i und F_j verlangt für die jetzt vorliegende Resultante die Vertauschung von $(F_i)_{x_k=0}$ und $(F_j)_{x_k=0}$; dabei geht R_{0k} in $(-1)^{N_k} R_{0k}$ und die Resultante selbst in

$$(-1)^N a_{kk}^{N_k} R_{0k}^{n}$$

über, dem zu beweisenden Satze entsprechend.

Der Produktsatz der Resultantentheorie.

§ 11. Es seien F_i' und F_i'' zwei allgemeine Formen $n_i'^{\text{ter}}$ und $n_i''^{\text{ter}}$ Dimension der Unbestimmten $x_1, \ldots, x_m$:

$$F_i' = \sum_{(g)} b_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}, \quad F_i'' = \sum_{(g)} c_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}.$$

Ersetzt man in dem allgemeinen Formensysteme $F_1, \ldots, F_{m+1}$ die Form F_i der Reihe nach durch die Formen $F_i' F_i''$, F_i' und F_i'' und nennt die entsprechend gebildeten Resultanten R, R', R'', so ist

$$R = R'R'',$$

der Produktsatz der Resultantentheorie.

Um den Satz zu beweisen, bedenke man, daß

$$R \equiv 0 \text{ (mod. } F_1, \ldots, F_{i-1}, F_i'F_i'', \ldots),$$

und auch

$$R \equiv 0 \text{ (mod. } F_1, \ldots, F_{i-1}, F_i', F_{i+1}, \ldots)$$
$$R \equiv 0 \text{ (mod. } F_1, \ldots, F_{i-1}, F_i'', F_{i+1}, \ldots)$$

ist. Demnach wird, da das Modulsystem aus „allgemeinen" Formen besteht, R durch R' und R'' teilbar. Nun sind R', R'' nicht nur irreduzibel, sondern auch nicht äquivalente Formen, denn sie enthalten verschiedene Reihen von Unbestimmten. Also ist R auch durch $R'R''$ teilbar:

$$R = AR'R'',$$

und A muß, wie aus der Dimension von R, R', R'' sich unmittelbar ergibt, eine rationale und ganze Zahl sein. Nun hat man endlich

$$R' = a_{11}^{N_1'} \cdots b_{ii}^{N_i'} \cdots a_{m+1,m+1}^{N_{m+1}'} + \cdots$$
$$R'' = a_{11}^{N_1''} \cdots c_{ii}^{N_i''} \cdots a_{m+1,m+1}^{N_{m+1}''} + \cdots$$
$$R = a_{11}^{N_1'+N_1''} \cdots (b_{ii}c_{ii})^{N_i'+N_i''} \cdots a_{m+1,m+1}^{N'm+1+N''m+1} + \cdots$$

und, wegen $N_i' = N_i''$, durch Vergleichung der Koeffizienten $A = 1$.

Wir werden insbesondere den Produktsatz für den Fall anzuwenden haben, wo sämtliche Formen F Produkte allgemeiner linearer Formen sind.

Die Resultante von $m + 1$ allgemeinen linearen Formen:

$$L_i = a_{i1}x_1 + \cdots + a_{im}x_m + a_{i,m+1}$$
$$(i = 1, \ldots, m + 1)$$

ist augenscheinlich die Determinante $|a_{ij}|$. Daß

$$|a_{ij}| \equiv 0 \text{ (mod. } L_1, \ldots, L_{m+1}),$$

wird in den Elementen der Determinantentheorie bewiesen. Diese Determinante enthält aber auch in ihrer Entwicklung

das Hauptglied $a_{11} \ldots a_{m+1,\,m+1}$ mit dem Koeffizienten 1 und ist also mit der Resultante identisch, wenn sie sich als irreduzible Form der Unbestimmten a erweist.

Daß $|a_{ij}|$ eine irreduzible Form der a darstellt, ist auch unabhängig von der Theorie der Resultanten durch den Schluß von $m-1$ auf m leicht klarzustellen. Diese Determinante ist, wie ihre Entwicklung zeigt, eine primitive Form und eine lineare Form jeder Reihe $a_{i1}, a_{i2}, \ldots, a_{im}$. Jeder echte Teiler d muß demnach wieder primitiv sein und wenigstens eine Reihe, z. B. $a_{i1}, \ldots, a_{im}$ nicht enthalten; denn sonst wäre der komplementäre Teiler d' (für den $dd' = |a_{ij}|$ wird) eine ganze Zahl, also gleich Eins, und d kein echter Teiler. Dann muß aber in

$$|a_{ij}| = \sum_{j=1}^{m} a_{1j} A_{1j}$$

$A_{11}, \ldots, A_{1m}$ durch d teilbar sein. Ist $m=2$, also $A_{11} = a_{22}$, $A_{12} = -a_{21}$, so sind dies irreduzible Größen ohne gemeinschaftlichen Teiler, also der supponierte Teiler ~ 1. Setzt man nun den Satz für $m-1$ als richtig voraus, so sind $A_{11}, \ldots, A_{1m}$ als Determinanten $m-1^{\text{ten}}$ Grades, in denen die Elemente durchaus verschiedene Unbestimmte sind, jedenfalls irreduzible Formen und auch nicht äquivalent, da z. B. A_{1r} die Unbestimmte a_{ir}, die in allen andern A_{1s} auftritt, gar nicht enthält. Es haben daher $A_{11}, \ldots, A_{1m}$ den größten gemeinschaftlichen Teiler 1; demnach ist $d \sim 1$ und der Satz bewiesen.

Es sei nun jedes F_i ein Produkt linearer Formen:

$$F_i = \prod_{\mu_i=1}^{n_i} \left(c_{i1}^{(\mu_i)} x_1 + c_{i2}^{(\mu_i)} x_2 + \cdots + c_{im}^{(\mu_i)} x_m + c_{i,m+1}^{(\mu_i)}\right),$$

dann wird durch wiederholte Anwendung des Produktsatzes:

$$\text{Res.}\,(F_1, \ldots, F_{m+1}) = \prod_{\mu_{m+1}=1}^{n_{m+1}} \cdots \prod_{\mu_1=1}^{n_1} \left| c_{ij}^{(\mu_i)} \right|_{(i,j=1,\ldots,m+1)},$$

eine Formel, die das Gesetz der Änderung der Resultante bei

Vertauschung von F_i mit F_j, oder x_i mit x_j aufs neue in Evidenz stellt, da hierbei in jeder Determinante zwei Spalten oder zwei Zeilen vertauscht werden, die Resultante selbst also mit $(-1)^N$ multipliziert wird.

Resultante eines Systems homogener Formen. Invarianteneigenschaft.

§ 12. Setzt man in dem allgemeinen Formensysteme

$$F_i(x_1, \cdots, x_m) \qquad (i = 1, \cdots, m+1)$$

$a_g^{(i)} x_{m+1}^{n_i - \Sigma g_j^{(i)}}$ an die Stelle von $a_g^{(i)}$, so entsteht das System der entsprechenden allgemeinen homogenen Formen (Kap. II. § 8):

$$\Phi_i(x_1, \ldots, x_{m+1}) \qquad (i = 1, \ldots, m+1);$$

ist ferner

$$R = \text{Res.} \begin{pmatrix} F_1, & F_2, & \ldots, & F_{m+1} \\ x_1, & x_2, & \ldots, & 1 \end{pmatrix},$$

so geht durch dieselbe Substitution die Identität

$$R = \sum_{i=1}^{m+1} H_i F_i,$$

da jedes Glied von R das Gewicht N hat, in

$$R x_{m+1}^N = \sum_{i=1}^{m+1} H_i \Phi_i$$

über. Setzt man

$$\left(\Phi_i(x_1, \ldots, x_{m+1})\right)_{x_j = 1} = F_i^{(j)},$$

so sind die $F_i^{(j)}$ wieder allgemeine Formen der Unbestimmten x mit Ausschluß von x_j, und es hat dabei nur eine gewisse gesetzmäßige Vertauschung der Koeffizienten $a_g^{(i)}$ stattgefunden. Die auf die Resultante bezügliche Identität wird dabei

$$R x_{m+1}^N = \sum_{i=1}^{m+1} H_i^{(j)} F_i^{(j)},$$

und aus dieser folgt in bekannter Weise (bei Benutzung der Kroneckerschen Substitution):

$$R \equiv 0 \pmod{F_1^{(j)}, \ldots, F_{m+1}^{(j)}}.$$

Nennt man R_j die Resultante des Systems $F_i^{(j)}$ nach den Unbestimmten x mit Ausschluß von x_j, so muß nun R durch R_j, und da die angewandte Schlußweise sich, wie unmittelbar zu sehn, umkehren läßt, auch R_j durch R teilbar sein, d. h. es ist

$$R_j = \pm R.$$

Von den Formen $F_i^{(j)}$ ausgehend, erhält man endlich für die Resultante auch

$$R x_j^N \equiv 0 \pmod{\Phi_1, \ldots, \Phi_{m+1}}$$

und nennt dementsprechend auch R die Resultante des homogenen Formensystems Φ_i, genauer in Bezug auf das Vorzeichen:

$$R = \text{Res.} \begin{pmatrix} \Phi_1, & \Phi_2, & \ldots, & \Phi_{m+1} \\ x_1, & x_2, & \ldots, & x_{m+1} \end{pmatrix}.$$

Auch bei dieser Definition bleibt die Grundeigenschaft der Resultante erhalten, indem die beiden Behauptungen

$$\Theta(a) \cdot x_i^\nu \equiv 0 \pmod{\Phi_1, \ldots, \Phi_{m+1}}$$
$$\Theta(a) \equiv 0 \pmod{R},$$

wobei $\Theta(a)$ irgend eine rationale und ganze Form der a bedeutet, dieselbe Tatsache aussprechen.

Ist $\Theta(a)$ durch R teilbar, so ist

$$\Theta(a) x_j^N \equiv 0 \pmod{\Phi_1, \ldots, \Phi_{m+1}},$$

während aus der ersten Behauptung

$$\Theta(a) \equiv 0 \pmod{F_1^{(j)}, \ldots, F_{m+1}^{(j)}},$$

mithin $\Theta(a) \equiv 0 \pmod{R}$ folgt. Dabei ist, wie man sieht, ν eine rationale und ganze Zahl, deren kleinster Wert sich aus der gegebenen Form $\Theta(a)$ bestimmt. Insbesondere hat man, wenn beiderseits die Glieder gleicher Dimension verglichen werden, eine spezielle Darstellung

$$\Theta(a)\, x_j^{\nu} = \sum_{i=1}^{m+1} H_i \Phi_i,$$

wo H_i eine homogene Form $\nu - n_i^{\text{ter}}$ Dimension der x ist und, wenn $\Theta(a)$ von 0 verschieden, auch $\nu \geqq n_i$ wird, da sonst H_i gleich Null wäre und dann auch $\Theta(a)$ verschwinden müßte. Dieser Schluß zeigt noch, daß aus

$$\Theta(a)\, x_j^{\nu} \equiv 0 \pmod{\Phi_1, \ldots, \Phi_{m+1}}$$

immer auch

$$\Theta(a)\, x_r^{\nu r} \equiv 0 \pmod{\Phi_1, \cdots, \Phi_{m+1}} \qquad (r = 1, \cdots, m+1)$$

folgt.

Es mögen nun die $m+1$ homogenen Formen

$$\Phi_i(x_1, \ldots, x_{m+1}) \qquad (i = 1, \ldots, m+1)$$

durch die (homogene) lineare Transformation mit unbestimmten Koeffizienten

$$x_j = \sum_{k=1}^{m+1} u_{jk} \bar{x}_k$$

in

$$\bar{\Phi}_i(\bar{x}_1, \ldots, \bar{x}_{m+1}) = \sum_{(g)} \bar{a}_g^{(i)}\, \bar{x}_1^{g_1^{(i)}} \ldots \bar{x}_{m+1}^{g_{m+1}^{(i)}}$$

übergehn, wo demnach die $\bar{a}_g^{(i)}$ rationale und ganze Formen der Unbestimmten $a_g^{(i)}$ und u_{jk} sind, und es sei

$$\bar{R} = \text{Res.}\begin{pmatrix} \bar{\Phi}_1, & \bar{\Phi}_2, & \ldots, & \bar{\Phi}_{m+1} \\ \bar{x}_1, & \bar{x}_2, & \ldots, & \bar{x}_{m+1} \end{pmatrix}.$$

Führt man in der entsprechenden Identität

$$\bar{R}\bar{x}_{m+1}^{N} = \sum H_i \Phi_i$$

die inverse Transformation

$$U\bar{x}_k = \sum_{j=1}^{m+1} U_{jk} x_j, \qquad U = |u_{ij}|$$

aus, so erhält man, da in den H_i nur eine Potenz von U als Nenner auftritt:

$$\bar{R}\, G \equiv 0 \pmod{\Phi_1, \ldots, \Phi_{m+1}},$$

wo G die a nicht enthält. Setzt man jetzt $x_{m+1} = 1$, so wird

$\bar{R}$ bei der Kroneckerschen Substitution verschwinden, und es ist demnach $\bar{R}$ durch R teilbar. Nun ist $\bar{a}_g^{(i)}$ eine homogene lineare Form der $a_g^{(i)}$; also $\bar{R}$ und R homogen und von gleicher Dimension in den $a_g^{(i)}$. Demnach wird

$$\bar{R} = RV$$

und V eine rationale und ganze Form der u_{ij}, zu deren Bestimmung irgend eine Spezialisation der $a_g^{(i)}$ ausreicht. Da für die Resultante eines Systems linearer Formen $V = U$ wird, kann man im allgemeinen Falle für F_i ein Produkt linearer Formen wählen (wie in § 11) und ersieht aus der dort gegebenen Darstellung die auch allgemein gültige Formel:

$$\bar{R} = R\,|u_{ij}|^N,$$

in der die s. g. Invarianteneigenschaft der Resultante ihren Ausdruck findet.

Systeme homogener Gleichungen.

§ 13. Die durch

$$R \equiv 0 \pmod{F_1^{(j)}, \ldots, F_{m+1}^{(j)}}$$

ausgedrückte Eigenschaft der Resultante zeigt unmittelbar, daß, wenn man die Größen $a_g^{(i)}$ als Veränderliche auffaßt, die Resultante verschwindet, sobald man den Größen $a_g^{(i)}$ solche Werte beilegt, für die wenigstens eines der Gleichungssysteme

$$F_1^{(j)} = 0, \quad F_2^{(j)} = 0, \cdots \qquad (j = 1, \ldots, m+1)$$

eine Lösung besitzt. Daß aber die Resultante auch nur in diesem Falle verschwindet, ist ein für die Theorie der Gleichungssysteme fundamentaler Satz, mit dem wir uns jetzt näher beschäftigen.

Man kann die $m+1$ Systeme von irgend welchen k Gleichungen $F_i^{(j)} = 0$ mit m Unbekannten in einfacher und für die geometrische Interpretation wichtiger Weise durch die Betrachtung des Systems von homogenen Gleichungen mit $m+1$ Unbekannten

$$\Phi_i(x_1, \ldots, x_{m+1}) = 0 \qquad (i = 1, \ldots, k)$$

zusammenfassen. Dabei soll jene Lösung, in der sämtliche Unbekannte den Wert 0 erhalten und die immer unabhängig von den Werten der Koeffizienten auftritt, ein für allemal ausgeschlossen werden.

Ist nun $\xi_1, \ldots, \xi_{m+1}$ irgend ein anderes Wurzelsystem, so ist, wenn λ eine ganz beliebige Größe bedeutet, auch $\lambda\xi_1, \ldots, \lambda\xi_{m+1}$ ein Wurzelsystem von $\Phi_i = 0$. Diese Wurzelsysteme wollen wir als eine „wirkliche" Lösung

$$x_1 : x_2 : \cdots : x_{m+1} = \xi_1 : \xi_2 \cdots : \xi_{m+1}$$

zusammenfassen, und demnach eine zweite Lösung $\eta_1, \ldots, \eta_{m+1}$ von der ersten als nicht verschieden ansehn, wenn

$$\xi_1 : \xi_2 : \cdots : \xi_{m+1} = \eta_1 : \eta_2 : \cdots : \eta_{m+1}.$$

Da mindestens eine der Größen ξ, z. B. ξ_j von 0 verschieden, gibt es einen und nur einen Wert λ_j für λ, so daß $\lambda_j\xi_j = 1$ wird, und $x_r = \lambda_j\xi_r$ ist ein Wurzelsystem der Gleichungen $F_i^{(\nu)} = 0$. Umgekehrt ergibt jedes Wurzelsystem von $F_i^{(\nu)} = 0$ eine Lösung von $\Phi_i = 0$, in welcher $\xi_j = 1$ ist.

Jene Lösungen von $\Phi_i = 0$, in denen $\xi_j = 0$ ist, pflegt man aus einfachen geometrischen Gründen als „im Unendlichen liegende" Lösungen von $F_i^{(\nu)} = 0$ zu bezeichnen; es ist dies eine Erweiterung des Begriffs der Lösung, durch welche die Ausnahmefälle in der Theorie des Systems $F_i = 0$ beseitigt werden; dies geschieht schon in den Elementen, wenn z. B. in dieser Weise der „unendlich ferne" Schnittpunkt zweier Geraden u. s. f. definiert wird (Kollineation).

Der zu beweisende Satz nimmt jetzt die folgende einfache Gestalt an:

Die Resultante des Systems

$$\Phi_i(x_1, \cdots, x_{m+1}) \qquad (i = 1, \cdots, m+1)$$

verschwindet dann und nur dann, wenn das Gleichungssystem $\Phi_i = 0$ eine wirkliche Lösung besitzt.

Daß im Falle des Vorhandenseins einer wirklichen Lösung die Resultante verschwindet, ist aus den Identitäten

$$Rx_j^N = \sum_{i=1}^{m+1} H_i^{(j)} \Phi_i$$

unmittelbar klar; es ist also nur die Umkehrung zu erörtern.

Dabei ist vor allem zu bemerken, daß die Dimension n_i der einzelnen Formen Φ_i mit diesen selbstverständlich gegeben, daß aber diese Formen, da für die $a_g^{(i)}$ spezielle Werte angenommen wurden, nicht mehr regulär zu sein brauchen. Wir wenden deshalb wieder die allgemeine (homogene) lineare Transformation

$$x_j = \sum_{k=1}^{m+1} u_{jk} \bar{x}_k$$

an, durch welche die Formen Φ_i in reguläre Formen $\bar{\Phi}_i$, die Resultante R in $\bar{R} = RU^N$ übergeht. Einer „wirklichen" Lösung von $\Phi_i = 0$ entspricht eine „wirkliche" Lösung von $\bar{\Phi}_i = 0$ und umgekehrt; R und $\bar{R}$ können nur zu gleicher Zeit verschwinden; es wird also genügen, wenn wir den Satz für das transformierte System beweisen.

Bildet man mit durchweg neuen unbestimmten Koeffizienten die homogenen Formen der $\bar{x}$:

$$V_1, \ldots, V_{m+1} \quad \text{und} \quad W_1, \ldots, W_{m+1},$$

deren Dimensionen $n - n_1, \ldots, n - n_{m+1}$ seien, wo n eine beliebige positive ganze Zahl bedeutet, die nur so zu wählen ist, daß alle $n - n_i \geqq 0$ sind, so werden

$$\sum_{i=1}^{m+1} V_i \bar{\Phi}_i \quad \text{und} \quad \sum_{i=1}^{m+1} W_i \bar{\Phi}_i$$

homogene Formen n^{ter} Dimension in den x; und die Gleichungen

$$\sum_{i=1}^{m+1} V_i \bar{\Phi}_i = 0, \quad \sum_{i=1}^{m+1} W_i \bar{\Phi}_i = 0$$

besitzen dann und nur dann eine wirkliche Lösung, wenn dies für $\bar{\Phi}_i = 0$ der Fall ist. Bildet man daher

$$\text{Res.}\begin{pmatrix} \sum_{i=1}^{m+1} V_i \bar{\Phi}_i & , & \sum_{i=1}^{m+1} W_i \bar{\Phi}_i \\ \bar{x}_1 & , & 1 \end{pmatrix},$$

so wird die notwendige und hinreichende Bedingung für die Existenz einer wirklichen Lösung von $\bar{\Phi}_i = 0$ sich dahin aussprechen lassen, daß ein Wertsystem $\bar{\xi}_2, \ldots, \bar{\xi}_{m+1}$, das nicht aus lauter Nullen besteht, vorhanden sein muß, für welches jene Resultante verschwindet. Für diese Werte gibt es jedenfalls (weil die Formen, deren Resultante wir bilden, regulär sind) einen zugehörigen Wert $\bar{\xi}_1$, so daß

$$\bar{\Phi}_i(\bar{\xi}_1, \ldots, \bar{\xi}_{m+1}) = 0$$

wird; wäre aber $\bar{\xi}_i = 0$ $(i = 2, \cdots, m+1)$, so müßte aus dem angeführten Grunde auch $\bar{\xi}_1 = 0$ sein.

Ordnet man jene Resultante nach den Potenzprodukten der in den V_i und W_i auftretenden Unbestimmten und nennt die Koeffizienten $\bar{\Phi}'_{i_1}(i_1 = 1, \ldots, k_1)$, so ist endlich jene Bedingung so zu fassen, daß das System homogener Gleichungen

$$\bar{\Phi}'_{i_1}(\bar{x}_2, \ldots, \bar{x}_{m+1}) = 0 \qquad (i_1 = 1, \ldots, k_1)$$

eine wirkliche Lösung besitzen muß. Dabei haben die Φ'_{i_1} nach ihrer Bildung die weitere Eigenschaft, daß

$$\Phi'_{i_1} \equiv 0 \ (\text{mod. } \bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}),$$

wie dies aus der entsprechenden Eigenschaft der Resultante durch Vergleichung der neben den einzelnen Potenzprodukten auftretenden Koeffizienten unmittelbar hervorgeht.

Bei genauer Wiederholung dieser Schlüsse gelangt man schließlich dazu, jene notwendige und hinreichende Bedingung so auszusprechen, daß das System homogener Gleichungen

$$\bar{\Phi}^{(m)}_{i_m}(\bar{x}_{m+1}) = 0 \qquad (i_m = 1, \ldots, k_m),$$

in dem

$$\bar{\Phi}^{(m)}_{i_m} \equiv 0 \ (\text{mod. } \bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1})$$

ist, eine wirkliche Lösung besitzen muß. Für die Gültigkeit

dieses Schlusses ist nur notwendig, daß das Formensystem $\bar{\Phi}_{i_k}^{(k)}$ durchweg aus regulären Formen bestehe. Dies ist aber schon durch die erstmalige Anwendung der allgemeinen linearen Transformation auf die Formen Φ_i gesichert. Wäre es nicht der Fall, so würde eine lineare Transformation zu regulären Formen führen; das durch eine solche erstrebte Ziel muß aber schon in jener allgemeinen Transformation erreicht sein, da jene spezielle Folge zweier linearer Transformationen in der allgemeinen als spezieller Fall enthalten ist.

Nun ist aber, als homogene Form einer Unbestimmten:

$$\bar{\Phi}_{m}^{(m)} = \varphi_{i_m}^{(m)} \bar{x}_{m+1}^{\nu_{i_m}},$$

folglich besitzt $\bar{\Phi}_i = 0$ dann und nur dann eine wirkliche Lösung, wenn die $\varphi_{i_m}^{(m)}$, die Formen der Unbestimmten u_{ij} sind, sämtlich verschwinden, und dabei ist

$$\varphi_{i_m}^{(m)} \bar{x}_{m+1}^{\nu_m} \equiv 0 \ (\text{mod. } \bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}) \ .$$

Um die Struktur der Größen $\varphi_{i_m}^{(m)}$ genauer zu erforschen, wiederholen wir dieselbe Reihe von Operationen an den Formen $\bar{\Phi}_i$, indem wir die Größen $a_g^{(i)}$ als Unbestimmte auffassen. Weil nun für jene speziellen Werte der $a_g^{(i)}$ die Formen regulär bleiben, und, da sie homogen sind, auch keine Erniedrigung der Dimension stattfindet, erhält man die früheren Formen immer dadurch, daß man in den allgemeinen $\bar{\Phi}_{i_m}^{(m)}$ die Werte der $a_g^{(i)}$ einsetzt. Nur der Fall, wo eine Form $\bar{\Phi}_{i_k}^{(k)}$ bei Einsetzung jener Werte identisch verschwindet, ist in dieser Schlußfolgerung nicht inbegriffen; aber auch in diesem Falle werden, wie unmittelbar zu sehn, aus den allgemein gebildeten Formen jene speziellen hervorgehn, und dabei nur eine Reihe weiterer Formen auftreten, die bei jener Spezialisation verschwinden.

Für ein beliebiges Gleichungssystem $\bar{\Phi}_i = 0$ erhält man mithin die notwendige und hinreichende Bedingung für die Existenz einer wirklichen Lösung in der Gestalt:

$$\varphi_{i_m}^{(m)} = 0 \qquad (i_m = 1, \ldots, k_m),$$

wo die $\varphi_{i_m}^{(m)}$ Formen der $a_g^{(i)}$ und u_{ij} sind, die also für die in Betracht kommenden speziellen Werte der $a_g^{(i)}$ verschwinden müssen.

Dabei haben aber die $\varphi_{i_m}^{(m)}$ als Formen der Unbestimmten $a_g^{(i)}$ die Eigenschaft, daß

$$\varphi_{i_m}^{(m)} \bar{x}_{m+1}^{\nu_m} \equiv 0 \ (\text{mod. } \bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}),$$

wo in dem hingeschriebenen Modulsysteme die $\bar{\Phi}_i$ wieder die allgemeinen Formen mit unbestimmten $a_g^{(i)}$ bedeuten. Daraus folgt wie früher, daß jedes $\varphi_{i_m}^{(m)}$ durch die Resultante $\bar{R}$ der allgemeinen Formen $\bar{\Phi}_i$ teilbar ist. Ist also $R = 0$, so wird auch jedes $\varphi_{i_m}^{(m)} = 0$, und es existiert eine wirkliche Lösung. Damit ist der ausgesprochene Satz bewiesen.

Bestimmte und unbestimmte gewöhnliche Systeme.

§ 14. Es sollen jetzt Systeme von m homogenen Gleichungen mit $m + 1$ Unbekannten

$$\Phi_i(x_1, \ldots, x_{m+1}) = 0 \qquad (i = 1, \ldots, m)$$

näher untersucht werden, deren Theorie nach dem vorhergehenden mit derjenigen von m nicht durchweg homogenen Gleichungen mit m Unbekannten, $F_i(x_1, \ldots, x_m) = 0$, zusammenfällt. Diese Systeme sollen, ohne daß wir auf die Bezeichnung gerade Gewicht legen, als „gewöhnliche" bezeichnet werden, im Gegensatze zu solchen, in denen die Anzahl der Gleichungen kleiner oder größer als m ist.

Die wichtigste Frage bezieht sich auf die Anzahl der verschiedenen Lösungen. Ist diese endlich, so soll das System bestimmt heißen, im entgegengesetzten Falle unbestimmt. Der Fall, daß gar keine wirkliche Lösung vorhanden ist, kann, wie sich ergeben wird, überhaupt nicht vorkommen.

Ist die Anzahl der verschiedenen wirklichen Lösungen endlich, z. B. n, so wird das durch die allgemeine lineare Transformation

$$x_j = \sum_{k=1}^{m+1} u_{jk} \bar{x}_k$$

erhaltene System

$$\bar{\Phi}_i(\bar{x}_1, \ldots, \bar{x}_{m+1}) = 0,$$

wie unmittelbar klar, auch n verschiedene wirkliche Lösungen besitzen, und in keiner davon wird ein $\bar{x}_k$ Null sein, da dies wegen

$$U\bar{x}_k = \sum_{j=1}^{m+1} U_{jk} x_j$$

nur dann der Fall sein kann, wenn $\sum_{j=1}^{m+1} U_{jk} x_j$ für das durch eine Lösung gegebene Wertsystem verschwindet. Seien nun die n verschiedenen Lösungen

$$\xi_{1r}, \xi_{2r}, \cdots, \xi_{m+1,r} \qquad (r = 1, \ldots, n),$$

wo die in einer Zeile stehenden Größen nicht sämtlich Null sind, so kann man beliebig viele Reihen von Größen (auch rationalen Zahlen) so bestimmen, daß

$$\sum_{j=1}^{m+1} a_{jk} \xi_{jr} \qquad (r = 1, \cdots, n;\ k = 1, \ldots, m+1)$$

nicht Null wird und auch die Determinante $|\, a_{jk} \,|_{(j,k=1,\ldots,m+1)}$ nicht verschwindet.

Aus der Auflösung der Gleichungen

$$|\, a_{jk} \,|\, \bar{\xi}_{kr} = \sum_{j=1}^{m+1} a_{jk} \xi_{jr} \qquad (k = 1, \ldots, m+1)$$

ergeben sich aber in den Formeln

$$\xi_{jr} = \sum_{k=1}^{m+1} b_{jk} \bar{\xi}_{kr}$$

solche Größen b_{jk} (die mit den a_{jk} auch rationale Zahlen sind), daß, wenn $u_{jk} = b_{jk}$ gesetzt wird, $\sum_{j=1}^{m+1} U_{jk} x_j$ in $\sum_{j=1}^{m+1} a_{jk} x_j$ übergeht. Es wird also keine der Größen

$$U\bar{\xi}_{kr} = \sum_{j=1}^{m+1} U_{jk} \xi_{jr} \qquad (k = 1, \cdots, m+1;\ r = 1, \cdots, n)$$

verschwinden, da dies auch dann nicht der Fall ist, wenn statt der Unbestimmten u_{jk} die Größen b_{jk} gesetzt werden.

Das transformierte System $\overline{\Phi}_i = 0$ hat demnach keine wirkliche Lösung, in der irgend ein $\bar{x}_k$ den Wert 0 annimmt, und daraus folgt unmittelbar, daß das System

$$(\overline{\Phi}_i)_{\bar{x}_{m+1}=0} = 0 \qquad (i = 1, \ldots, m)$$

überhaupt keine wirkliche Lösung besitzt (selbstverständlich unter der Voraussetzung, daß für das vorgelegte System nur eine endliche Anzahl wirklicher Lösungen vorhanden ist). Aus dieser Tatsache folgt endlich auch, daß in diesem Falle (nach dem in § 13 bewiesenen Satze)

$$\overline{R}_{m+1}(u) = \text{Res.}\begin{pmatrix}(\overline{\Phi}_1)_{\bar{x}_{m+1}=0}, \ldots, (\overline{\Phi}_m)_{\bar{x}_{m+1}=0} \\ \bar{x}_1 \quad , \ldots, \quad \bar{x}_m\end{pmatrix}$$

von Null verschieden sein muß.

Hat andrerseits das vorgelegte System unendlich viele verschiedene wirkliche Lösungen, so gibt es unter diesen auch unendlich viele wirkliche Lösungen, in denen $\bar{x}_{m+1}$ nicht Null wird; diese verschiedenen Lösungen von $\overline{\Phi}_i = 0$ entsprechen immer auch verschiedenen Lösungen von $(\overline{\Phi}_i)_{\bar{x}_{m+1}=1} = 0$; und die Glieder höchster Dimension in $(\overline{\Phi}_i)_{\bar{x}_{m+1}=1}$ sind einfach die Glieder von $(\overline{\Phi}_i)_{\bar{x}_{m+1}=0}$.

Bildet man die Resultante des Formensystems

$$-\bar{x}_j + z, (\overline{\Phi}_i)_{\bar{x}_{m+1}=1} \qquad (i = 1, \ldots, m),$$

so wird diese nach ihren Grundeigenschaften, nach Potenzen von z geordnet:

$$\overline{R}_{m+1} z^N + \cdots,$$

wo $N = n_1, \ldots, n_m$, und

$$\overline{R}_{m+1} z^N + \ldots \equiv 0 \left(\text{mod.}\, z - \bar{x}_j, (\overline{\Phi}_i)_{\bar{x}_{m+1}=1}, \ldots, (\overline{\Phi}_m)_{\bar{x}_{m+1}=1}\right).$$

Ist also $\bar{\xi}_1, \ldots, \bar{\xi}_m$ eine Lösung des Systems $(\overline{\Phi}_i)_{x_{m+1}=1} = 0$, und setzt man weiter in dem Modulsystem

$$\bar{x}_j = \bar{\xi}_j, \; z = \bar{\xi}_j,$$

so wird

$$\bar{R}_{m+1}\bar{\xi}_j^N + \cdots = 0,$$

und es kann, wenn $\bar{R}_{m+1}$ nicht Null ist, $\bar{\xi}_j$ höchstens N verschiedene Werte erhalten.

Wir haben damit folgenden Satz gewonnen:

Das System hat eine endliche oder unendliche Anzahl verschiedener wirklicher Lösungen, je nachdem die Form $\bar{R}_{m+1}(u)$ von Null verschieden oder gleich Null ist.

Dabei ist der Satz sogleich in der schärferen Fassung zu verstehen, daß jene endliche Anzahl niemals Null, also zumindest eine wirkliche Lösung vorhanden ist, wie dies aus der in § 16 zu entwickelnden Theorie jener Systeme, für welche $\bar{R}_{m+1}(u)$ nicht Null ist, unmittelbar hervorgehen wird.

Noch sei bemerkt, daß homogene Gleichungen mit $m+1$ Unbekannten „im allgemeinen" eine endliche Anzahl von verschiedenen Lösungen besitzen. Schreibt man nämlich $\bar{R}_{m+1}(u)$ ausführlich

$$\bar{R}_{m+1}(u) = A_0 U_0 + A_1 U_1 + \cdots,$$

wo die U Potenzprodukte der u_{jk} bedeuten und die A rationale und ganze Formen der $a_g^{(i)}$ sind, so ist dies dann und nur dann nicht der Fall, wenn die Koeffizienten $a_g^{(i)}$ den Gleichungen

$$A_0 = 0, \; A_1 = 0, \ldots$$

genügen*).

§ 15. Jene Festsetzungen, die im vorhergehenden Paragraphen für das homogene System $\Phi_i(x_1, \ldots, x_{m+1}) = 0$, $(i = 1, \ldots, m)$ erfolgten, können unmittelbar auf das nicht homogene System

*) Man kann leicht die Analogie verfolgen, die zwischen den Entwicklungen des vorigen und jetzigen Kapitels besteht. Dabei ist aber auch der prinzipielle Gegensatz zu beachten, nach dem dort die Anzahl der Gleichungen nicht durch die Anzahl der Unbekannten beschränkt war, während jetzt andrerseits durch die Hinzunahme der „im Unendlichen" liegenden Wurzeln das zu behandelnde Problem wieder eine Erweiterung erfuhr.

$$F_i(x_1, \ldots, x_m) = 0 \quad (i = 1, \ldots. m)$$

übertragen werden.

Auch dieses „gewöhnliche" System (in welchem die Anzahl der Unbekannten mit der Anzahl der Gleichungen übereinstimmt) soll bestimmt, bez. unbestimmt heißen, je nachdem die Anzahl der verschiedenen wirklichen Lösungen — Wurzelsysteme und „im Unendlichen liegende" Lösungen — endlich, bez. unendlich ist.

Wir kennen nach § 14 die notwendige und hinreichende Bedingung dafür, daß ein solches System bestimmt sei. Es wird aber zweckmäßig sein, die Fragestellung nochmals aufzunehmen und so durchzuführen, daß wir die allgemeine lineare Transformation der Formen Φ_i (d. h. geometrisch gesprochen, das Prinzip der Kollineation) nicht benutzen. Im übrigen soll auch jetzt nur die Theorie der Resultanten — und nicht die allgemeine Theorie der Elimination — benutzt werden.

Zu diesem Zwecke fügen wir den Formen $F_i(x_1, \ldots, x_m)$ noch die weitere Form

$$-\sum_{j=1}^{m} t_j x_j + z$$

hinzu und bezeichnen die Resultante des so entstandenen Formensystems

$$\text{Res.} \begin{pmatrix} F_1, \ldots, F_m, & z - \sum_{j=1}^{m} t_j x_j \\ x_1, \ldots, x_m, & 1 \end{pmatrix}$$

als Eliminante des Systems F_i (in Bezug auf $z = \sum_{j=1}^{m} t_j x_j$). Diese ist, ausführlich geschrieben:

$$E(z; t_1, \ldots, t_m) = R_{m+1} z^N + R'_{m+1} z^{N-1} + \ldots.$$

Versteht man unter φ_i den Komplex der Glieder höchster (n_i^{ter}) Dimension in F_i, also eine homogene Form, so ist in jener Eliminante

$$R_{m+1} = \text{Res.} \begin{pmatrix} \varphi_1, \ldots, \varphi_m \\ x_1, \ldots, x_m \end{pmatrix},$$

während R'_{m+1} u. s. w. auch die Unbestimmten $t_1, \ldots, t_m$ enthalten.

Man hat dann folgenden Satz:

Das System $F_i(x_1, \ldots, x_m) = 0$, $(i = 1, \ldots, m)$ ist bestimmt oder unbestimmt, je nachdem die als Eliminante bezeichnete Form $E(z; t_1, \ldots, t_m)$ von Null verschieden oder gleich Null ist.

Ist nämlich $\xi_1, \ldots, \xi_m$ ein Wurzelsystem von $F_i = 0$, und sind $z, t_1, \ldots, t_m$ irgend welche Größen, die der Gleichung

$$z - \sum_{j=1}^{m} t_j \xi_j = 0$$

genügen, so wird die Form E — ihrer Bedeutung als Resultante gemäß — für jedes solche Wertsystem von $z, t_1, \ldots, t_m$ verschwinden. Daraus folgt aber nach den in Kap. V. § 7 benutzten Methoden oder auch einfacher nach dem in der Fußnote gegebenen Hilfssatze*), daß E durch $z - \sum_{j=1}^{m} t_j \xi_j$ teilbar ist.

---

*) Statt der im Text citierten Entwicklungen der allgemeinen Eliminationstheorie genügt der folgende einfache Hilfssatz (nicht nur an dieser Stelle, sondern auch bei den später öfter anzuwendenden analogen Schlüssen):

Ist $P(z_1, z_2, \ldots)$ irgend eine in dem orthoiden Bereiche (A) irreduzible Form, und die von 0 verschiedene Form $\Phi(z_1, z_2, \ldots)$ gleich Null für jedes aus (A) entnommene Wertsystem $\zeta_1, \zeta_2, \ldots$, das $P(\zeta_1, \zeta_2, \ldots) = 0$ gibt, so muß Φ durch P teilbar sein.

Jedenfalls muß eine der Unbestimmten, z. B. z_1, in Φ und P wirklich enthalten sein, sonst kann man unmittelbar ein Wertsystem $\zeta_1, \zeta_2, \ldots$ bilden, für das P Null wird und Φ nicht verschwindet. Dann muß aber, wenn Φ nicht durch P teilbar ist, die Resultante von Φ und P nach z_1, die mit Z bezeichnet werden möge, von Null verschieden sein, und man hat die Relation

$$Z = Z_1 \Phi + Z_2 P.$$

Man kann aber für $z_2, z_3, \ldots$ solche Werte wählen, daß Z und der Koeffizient der höchsten Potenz von z_1 in P von Null verschieden werden. Diesen Werten $\zeta_2, \zeta_3, \ldots$ entspricht aber jedenfalls ein Wert $z_1 = \zeta_1$, für den $P = 0$ wird; und für dieses Wertsystem wäre $Z_1 \Phi = Z$, also im Gegensatze zur Annahme $Z_1 \Phi$ und demnach auch P von Null verschieden.

Ebenso wird die Form E — wieder infolge ihrer Bedeutung als Resultante — für jedes Wertsystem $t_1, \ldots, t_m$ verschwinden, das der Gleichung

$$\sum_{j=1}^{m} t_j \eta_j = 0$$

genügt, wenn

$$x_1 : \cdots : x_m = \eta_1 : \cdots : \eta_m$$

irgend eine im Unendlichen liegende wirkliche Lösung von $F_i = 0$ ist. In diesem Falle muß also E durch $\sum_{j=1}^{m} t_j \eta_j$ teilbar sein.

Den verschiedenen Lösungen von $F_i = 0$ entsprechen demnach verschiedene, auch nicht äquivalente lineare Teiler von E. Ist aber E nicht Null, so besitzt diese Form nur eine endliche Anzahl linearer Teiler, und es muß demnach für den Fall eines unbestimmten Systems jedenfalls die Eliminante identisch verschwinden.

Um jetzt den Fall eines bestimmten Systems näher zu untersuchen, für welches sowohl die Anzahl der Wurzelsysteme, als auch diejenige der im Unendlichen liegenden Lösungen endlich ist, seien die Wurzelsysteme eines solchen Systems, soweit solche überhaupt vorhanden sind:

$$\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk} \qquad (k = 1, \ldots, \mu)$$

und seine im Unendlichen liegenden verschiedenen wirklichen Lösungen wieder, soweit solche vorhanden sind:

$$x_1 : \cdots : x_m = \eta_{1l} : \cdots : \eta_{ml} \qquad (l = \mu + 1, \ldots, \nu).$$

Bildet man aus diesen die Formen:

$$z - \sum_{j=1}^{m} t_j \xi_{jk}, \quad \sum_{j=1}^{m} t_j \eta_{jl} \quad (k = 1, \ldots, \mu;\ l = \mu + 1, \ldots, \nu),$$

so gibt es jedenfalls Wertsysteme $\zeta, \tau_1, \ldots, \tau_m$ von der Beschaffenheit, daß keine dieser Formen verschwindet, wenn in ihnen $\zeta, \tau_1, \ldots, \tau_m$ statt $z, t_1, \ldots, t_m$ gesetzt wird. Demnach besitzt das Gleichungssystem

$$F_i = 0, \quad \xi - \sum_{j=1}^{m} \tau_j x_j = 0$$

keine Lösung, und es muß demnach $E(\xi; \tau_1, \ldots, \tau_m)$ von Null verschieden sein. Es kann also $E(z, t_1, \ldots, t_m)$ nicht identisch verschwinden, und damit ist der oben ausgesprochene Satz vollständig bewiesen.

Auf Grundlage dieser Betrachtungen kann noch die Gestalt der Eliminante eines bestimmten Systems genauer präcisiert werden:

Gehören zu den für diesen Fall gebildeten linearen Teilern der Eliminante die Exponenten c_k, bez. c_l, so wird die Eliminante:

$$E(z, t_1, \ldots, t_m) = Q \prod_{k=1}^{\mu} \left(z - \sum_{j=1}^{m} \xi_{jk} t_j \right)^{c_k} \prod_{l=\mu+1}^{\nu} \left(\sum_{j=1}^{m} \eta_{jl} t_j \right)^{c_l},$$

und in dieser die Größe Q, die jedenfalls von Null verschieden sein muß, weil das System ein bestimmtes ist, ein von $z, t_1, \ldots, t_m$ unabhängiger Koeffizient.

Wäre nämlich Q eine wirkliche Form von $z, t_1, \ldots, t_m$, so müßte jedenfalls einer ihrer irreduzibeln Teiler P dieselbe Eigenschaft besitzen. Dann gibt es aber ein Wertsystem $\xi, \tau_1, \ldots, \tau_m$, für welches P verschwindet, während jene linearen Teiler sämtlich von Null verschiedene Größen sind. Im entgegengesetzten Falle müßte das Produkt jener linearen Teiler durch P teilbar sein, was nach der für die c_k und c_l festgesetzten Bedeutung nicht möglich ist. Für jenes Wertsystem $\xi, \tau_1, \ldots, \tau_m$ verschwindet also Q, während die linearen Teiler von Null verschieden sind. Es gäbe also eine Lösung des Systems

$$F_i = 0, \quad -\sum_{j=1}^{m} \tau_j x_j + \xi = 0,$$

der ein neuer linearer Teiler von Q entsprechen müßte. Das ist aber nicht möglich, wenn jene Aufzählung der Lösungen, wie vorausgesetzt wurde, eine vollständige ist.

Man ersieht hieraus noch, daß ein bestimmtes System $F_i = 0$ dann und nur dann ein Wurzelsystem besitzt, wenn die Eliminante die Unbestimmte z wirklich enthält*).

Die Wurzelsysteme können in diesem Falle durch Zurückführung auf Gleichungen mit einer Unbekannten in einfachster Weise bestimmt werden.

Bildet man den größten gemeinschaftlichen Teiler von E und $\frac{\partial E}{\partial z}$ und entfernt ihn aus E, so erhält man

$$\varrho(z; t_1, \ldots, t_m) = A \prod_{k=1}^{m} (z - \Sigma t_j \xi_{jk}),$$

wo A von den t unabhängig ist und die Discriminante von ϱ eine von 0 verschiedene Form der t wird. Man kann ferner $t_s = a_s$ so bestimmen, daß z. B. die a_s rationale und ganze Zahlen sind, und Dscr. $\varrho(z; a_1, \ldots, a_m)$ von Null verschieden ist.

Da aber

$$[\varrho(z; t_1, \ldots, t_m)]_{z=\sum_{j=1}^{m} t_j \xi_{jk}}$$

als Form der t Null ist, muß auch die Derivierte nach t_j verschwinden, d. h.

$$\left[\frac{\partial \varrho}{\partial z}\right]_{z=\sum_{j=1}^{m} t_j \xi_{jk}} \xi_{jk} + \left[\frac{\partial \varrho}{\partial t_j}\right]_{z=\sum_{j=1}^{m} t_j \xi_{jk}} = 0$$

sein.

Setzt man daher

$$t_s = a_s, \quad z = \xi_k = \Sigma a_j \xi_{jk},$$

was durch das Zeichen $[\ldots]_a^{(k)}$ angedeutet werden soll, so bestimmt die Gleichung

$$\varrho(z; a_1, \ldots, a_m) = 0$$

*) Die Anzahl der Wurzelsysteme kann endlich und von Null verschieden sein, auch wenn die Eliminante Null ist; dies zeigt schon das einfache Beispiel des Systems:

$$x_1 = 0, \quad x_2(x_1 + 1) = 0, \quad x_3(x_1 + 1) = 0.$$

geradezu die Größen $\xi_k (k = 1, \ldots, \nu)$, und darauf

$$\left[\frac{\partial \varrho}{\partial z}\right]_a^{(k)} \xi_{jk} + \left[\frac{\partial \varrho}{\partial t_j}\right]_a^{(k)} = 0, \qquad (k = 1, \cdots, \nu)$$

die Größen ξ_{jk} durch rationale Operationen aus ξ_k; denn es kann $\left[\frac{\partial \varrho}{\partial z}\right]_a^{(k)}$ niemals verschwinden; sonst wäre nämlich im Gegensatze zur Bildung der Gleichung $\varrho(z; a_1, \ldots, a_m) = 0$ die Größe $z = \xi_k$ keine einfache, sondern eine mehrfache Wurzel dieser Gleichung.

Diese Darstellung definiert endlich auch die Multiplizität des Wurzelsystems $\xi_{1k}, \ldots, \xi_{mk}$ durch den Exponenten c_k, der dem linearen Faktor $z - \Sigma t_j \xi_{jk}$ in E zukommt; diesem entsprechend bezeichnet man das Wurzelsystem $\xi_{1k}, \ldots, \xi_{mk}$ als c_k-faches; oder sagt auch, daß die Größen $\xi_{1k}, \ldots, \xi_{mk}$ in diesem Falle c_k zusammenfallende Wurzelsysteme darstellen. Ganz ähnlich ergeben die Exponenten c_l die Multiplizität der im Unendlichen liegenden Lösungen.

§ 16. Wir knüpfen wieder an die Entwicklungen des § 14 an und untersuchen das System

$$\Phi_i(x_1, \ldots, x_{m+1}) = 0 \qquad (i = 1, \ldots, m)$$

unter der Voraussetzung, daß es nur eine endliche Anzahl wirklicher Lösungen besitzt, also die Resultante der Formen $(\overline{\Phi}_i)_{\bar{x}_{m+1}=0}$, die wie früher mit $\overline{R}_{m+1}(u)$ bezeichnet wird, von Null verschieden ist*).

Da sich bei einer homogenen linearen Transformation an der Fragestellung nichts ändert, kann man wie früher auf das System

$$\overline{\Phi}_i(\bar{x}_1, \ldots, \bar{x}_{m+1}) = 0$$

*) Für den Fall unendlich vieler wirklicher Lösungen tritt die im vorigen Kapitel entwickelte allgemeine Eliminationstheorie ein. Dabei ergeben sich insbesondere wichtige Gesichtspunkte, wenn man die im Unendlichen liegenden Lösungen von den endlichen sondert, d. h. einmal $x_{m+1} = 0$, das andre Mal $x_{m+1} = 1$ setzt, was selbstverständlich alle Lösungen umfaßt.

übergehn und dabei die Größen u_{ij} als Unbestimmte betrachten, oder aber auch diesen bestimmte (auch rationale und ganzzahlige) Werte zuschreiben, für welche $|u_{ij}|$ und $\bar{R}_{m+1}(u)$ nicht Null sind.

Da nun für eine wirkliche Lösung $\bar{x}_{m+1}$ niemals Null wird, kann man $\bar{x}_{m+1}$ gleich Eins setzen (oder, was auf dasselbe hinauskommt, den Nenner $\bar{x}_{m+1}^{n_i}$ hinzufügen und $\frac{\bar{x}_1}{\bar{x}_{m+1}}, \frac{\bar{x}_2}{\bar{x}_{m+2}}, \cdots$ als Unbekannte ansehn).

Das Gleichungssystem

$$(\bar{\Phi}_i)_{\bar{x}_{m+1}=1} = 0$$

ordnet sich also dem im vorhergehenden Paragraphen untersuchten Falle ein und gibt mit der Eliminante die Gleichung

$$\bar{R}_{m+1}(u)\, z^N + \bar{R}^{(1)}_{m+1}(u)\, z^{N-1} + \cdots + \bar{R}^{(N)}_{m+1} = 0,$$

aus der sich sämtliche Lösungen bestimmen.

Diese drückt das s. g. Bezoutsche Theorem aus, nach dem m homogene Gleichungen mit $m+1$ Unbekannten entweder unendlich viele oder genau $N = n_1 \ldots n_m$ wirkliche Lösungen besitzen, wenn jede solche Lösung so oft gezählt wird, als es ihre in § 15 definierte Multiplizität angibt.

Sind die u so gewählt, daß $\bar{R}_{m+1}(u)$ von Null verschieden, so geben sämtliche wirkliche Lösungen auch endliche Wurzelsysteme; für jene algebraische Mannigfaltigkeit homogener linearer Transformationen, deren Koeffizienten u_{ij} so gewählt sind, daß

$$\bar{R}_{m+1}(u) = 0, \ldots, R^{(k-1)}_{m+1} = 0$$

ist, liegen k wirkliche Lösungen „im Unendlichen", d. h. für diese ist $\bar{x}_{m+1} = 0$. Dies kann auch für sämtliche Lösungen der Fall sein, wenn $\bar{R}^{(N)}_{m+1}$ allein von Null verschieden ist.

Daß sämtliche Koeffizienten der Eliminante verschwinden, ohne daß $|u_{ij}| = 0$ ist, tritt dann und nur dann ein, wenn das System unendlich viele verschiedene wirkliche Lösungen besitzt.

§ 17. Es sollen wieder die Formen

$$F_i(x_1, \ldots, x_m) = \sum_{(g)} a_g^{(i)} x_1^{g_1} \ldots x_m^{g_m}$$

allgemeine Formen n_i^{ter} Dimension sein; insbesondere schreiben wir

$$F_i = \varphi_i + \cdots,$$

wo φ_i den Komplex der Glieder n_i^{ter} Dimension in F_i, also eine „allgemeine" homogene Form n_i^{ter} Dimension bedeutet. Dann ist

$$R_{m+1} = \text{Res.} \begin{pmatrix} \varphi_1, \ldots, \varphi_m \\ x_1, \ldots, x_m \end{pmatrix}$$

von Null verschieden, und das System hat N wirkliche Lösungen, von denen keine im Unendlichen liegt, also auch N Wurzelsysteme. Daß diese auch sämtlich verschieden sind, kann man in einfachster Weise durch irgend ein spezielles Beispiel erhärten, in dem die Größen $a_g^{(i)}$ so gewählt sind, daß die Formen F_i keine Erniedrigung der Dimension erfahren, und dabei doch das Gleichungssystem $F_i = 0$ genau N voneinander verschiedene Wurzelsysteme besitzt. Ein solches Beispiel bietet das System

$$x_1^{n_1} = x_2, \; x_2^{n_2} = x_3, \; \ldots, \; x_i^{n_i} = x_{i+1}, \; \ldots, \; x_m^{n_m} = 1,$$

dem wir dann und nur dann genügen, wenn x_1 gleich irgend einer N^{ten} Einheitswurzel gesetzt wird, und für $x_2, \ldots, x_m$ die aus der ersten, zweiten, ... Gleichung resultierenden Werte genommen werden.

Fügt man dem Systeme

$$F_i = 0 \qquad (i = 1, \ldots, m)$$

die weitere Gleichung

$$F_{m+1} + z = 0$$

hinzu (in der F_{m+1} eine allgemeine Form von der Dimension n_{m+1} bedeutet), so wird die Resultante der Formen F_i und $F_{m+1} + z$ (nach § 5 und 9):

$$R_{m+1}^{n_{m+1}} z^N + \cdots + R,$$

da keine unendlichen Lösungen existieren, dann und nur dann Null, wenn für ein Wurzelsystem von $F_i = 0$ auch $z + F_{m+1} = 0$ wird.

Bezeichnen wir also die N Wurzelsysteme von $F_i = 0$ mit

$$\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk}, \qquad (k = 1, \ldots, N)$$

wo die ξ bestimmte algebraische Funktionen der $a_g^{(i)}$ sind, so wird jene Resultante dann und nur dann Null, wenn z einen der Werte

$$-F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}) \qquad (k = 1, \ldots, N)$$

annimmt. Diese Werte sind, da die Koeffizienten von F_{m+1} wieder neue Unbestimmte sind, untereinander durchaus verschieden; denn aus

$$F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}) = F_{m+1}(\xi_{1l}, \ldots, \xi_{ml})$$

würde durch Vergleichung der Koeffizienten der linearen Glieder

$$\xi_{1k} = \xi_{1l}, \ldots, \xi_{mk} = \xi_{ml}$$

folgen, was, wie eben bewiesen wurde, nicht stattfindet.

Die Gleichung

$$R_{m+1}^{n_{m+1}} z^N + \cdots + R = 0$$

hat mithin genau die N voneinander verschiedenen Wurzeln $-F_{m+1}(\xi_{1k}, \ldots, \xi_{mk})$, und es ist demnach

$$R = R_{m+1}^{n_{m+1}} \prod_{k=1}^{N} F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}).$$

Andrerseits geht die Resultante der Formen $F_i, F_{m+1} + z$, wenn $z = 0$ gesetzt wird, da dies mit keiner Erniedrigung der Dimension verbunden ist, in die Resultante von $F_1, \ldots, F_{m+1}$ über, und diese ist demnach R. Man erhält also

$$\text{Res.}\begin{pmatrix} F_1, \ldots, F_m, F_{m+1} \\ x_1, \ldots, x_m, \quad 1 \end{pmatrix} = R_{m+1}^{n_{m+1}} \prod_{k=1}^{N} F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}),$$

wo noch

$$R_{m+1} = \text{Res.}\begin{pmatrix} \varphi_1, \ldots, \varphi_m \\ x_1, \ldots, x_m \end{pmatrix}.$$

Es ist dies die von Poisson*) gegebene Darstellung der Resultante, die sich unmittelbar als Verallgemeinerung der für die Resultante zweier Formen in Kap. III. § 24 gegebenen Gestalt erweist. Dabei sind die Größen ξ_{jk} algebraische Funktionen der in den allgemeinen Gleichungen $F_i = 0$ auftretenden unbestimmten Koeffizienten $a_g^{(i)}$. Insofern es sich um Gleichungen mit bestimmten Koeffizienten handelt, ist diese Gestalt der Resultante wieder eine symbolische, da zuerst die Umrechnung in die frühere Gestalt vorausgesetzt wird.

Diese Poissonsche Darstellung der Resultante führt zu einer Erweiterung des Begriffs der symmetrischen Form, mit welcher wir uns nun näher beschäftigen müssen, da sie einen tieferen Einblick in diese Bildungen gestattet und insbesondere die Untersuchung der s. g. Discriminante wesentlich erleichtert.

Symmetrische Formen von mehreren Größensystemen**).

§ 18. Es seien

$$x_{ij} \quad (i = 1, \ldots, m;\ j = 1, \ldots, n)$$

mn Unbestimmte, von denen die in einer Spalte stehenden

$$x_{1j}, x_{2j}, \ldots, x_{mj}$$

je ein „System", insbesondere die soeben hingeschriebenen das System (j) bilden. Eine Vertauschung der Systeme (j) und (k) bedeutet demnach eine solche Vertauschung der Unbestimmten, bei welcher x_{ij} und x_{ik} für jedes i zugleich vertauscht werden. Jede mögliche Vertauschung der gegebenen n Systeme wird demnach durch ein Symbol

*) „Sur l'élimination dans les équations algébriques." Journal de l'école polytechnique, Tome IV. Cah. 11. pag. 199.

**) Die Theorie dieser Formen, die bis auf Waring zurückzuführen ist, wurde zum ersten Male von Schläfli genauer dargelegt: „Über die Resultante eines Systems mehrerer algebraischer Gleichungen" (Denkschr. d. kais. Akad. d. Wiss. in Wien. Math.-nat.-wiss. Cl. IV. Bd. 2. Abt. 1852).

$$\begin{pmatrix} (1), & (2), & \ldots, & (n) \\ (j_1), & (j_2), & \ldots, & (j_n) \end{pmatrix}$$

bezeichnet werden können, wo $j_1, j_2, \ldots, j_n$ die Zahlen $1, \ldots, n$ in einer beliebigen Anordnung bedeuten.

Eine symmetrische Form der n Systeme x_{ij} ist eine solche, die bei jeder Vertauschung der Systeme ungeändert bleibt.

Jede solche symmetrische Form besteht der Natur der Sache nach aus Gliedern von der Gestalt AX, wo A eine Größe jenes holoiden Bereichs ist, dem die Form entstammt, und X ein Potenzprodukt der x_{ij}, also ausführlich

$$X = x_{1j_1}^{a_{11}} \ldots x_{mj_1}^{a_{m1}} x_{1j_2}^{a_{12}} \ldots x_{mj_2}^{a_{m2}} \ldots x_{1j_k}^{a_{1k}} \ldots x_{mj_k}^{a_{mk}}$$

ist, und $k \leqq n$. Wendet man auf dieses Potenzprodukt alle möglichen Vertauschungen der n Systeme an und bildet die Summe aller so auftretenden verschiedenen Potenzprodukte, so ist diese Summe, die kurz mit

$$\Sigma X$$

bezeichnet werden möge, eine symmetrische Form der x_{ij}; denn zwei verschiedene Potenzprodukte ergeben bei einer solchen Vertauschung wieder verschiedene Potenzprodukte; die Summe aller verschiedenen Potenzprodukte bleibt also bis auf die Anordnung ungeändert.

Die durch ein Potenzprodukt X in dieser Weise definierte symmetrische Form ΣX von besonders einfacher Struktur wird als typische symmetrische Form oder auch kurz als „Type“ bezeichnet; und es ist unmittelbar klar, daß jede symmetrische Form sich in der Gestalt

$$A_0 T_0 + A_1 T_1 + \cdots + A_s T_s$$

schreiben läßt, wo $T_0, T_1, \ldots, T_s$ verschiedene Typen, T_0 insbesondere 1 bedeutet, und $A_0, A_1, \ldots$ Koeffizienten der vorgelegten Form sind.

Unter den Typen erwähnen wir zuerst die elementaren symmetrischen Formen, die in Bezug auf jedes Größen-

system $x_{1j}, \ldots, x_{mj}$ linear sind, also ausführlich geschrieben von der Gestalt

$$\sum_{(j)} x_{r_1 j_1} x_{r_2 j_2} \cdots x_{r_k j_k}$$

sind, wo $k \leqq n$, $j_1, \ldots, j_k$ voneinander verschiedene k Zahlen aus der Reihe $1, \ldots, n$ bedeuten, und endlich $r_1, \ldots, r_k$ irgend welche gleiche oder verschiedene Zahlen aus der Reihe $1, \ldots, m$ sind. Die Anzahl der elementaren symmetrischen Formen k^{ter} Dimension wird durch die Anzahl der Glieder in dem als Form der t gefaßten Ausdrucke

$$(t_1 x_{11} + t_2 x_{21} + \cdots + t_m x_{m1}) \cdots (t_1 x_{1k} + t_2 x_{2k} + \cdots + t_m x_{mk})$$

gegeben, indem als Koeffizient eines Potenzproduktes $t_{r_1} \ldots t_{r_k}$ ein Ausdruck von der Gestalt

$$x_{r_1 1} x_{r_2 2} \cdots x_{r_k k} + \cdots$$

auftritt, ferner die verschiedenen Potenzprodukte und die hingeschriebenen ersten Glieder dieser Ausdrücke, und dann wieder diese ersten Glieder und die verschiedenen elementaren symmetrischen Formen k^{ter} Dimension sich gegenseitig eindeutig entsprechen. Es ist demnach die Anzahl der elementaren symmetrischen Formen k^{ter} Dimension (Kap. II. § 8)

$$\binom{m+k-1}{k},$$

und die Anzahl sämtlicher elementaren symmetrischen Formen

$$\sum_{k=1}^{n} \binom{m+k-1}{k} = \binom{m+n}{n} - 1.$$

Ist die Anzahl der in einem Systeme enthaltenen Größen $m = 1$, so erhält man die elementaren symmetrischen Formen einer Größenreihe $x_{11}, x_{12}, \ldots, x_{1n}$ im Sinne der Kap. II. § 10 entwickelten Theorie, die sich als spezieller Fall diesen Erörterungen einfügt. Die Anzahl der elementaren symmetrischen Formen ist also nur dann gleich der Anzahl der Unbestimmten, wenn $m = 1$, in jedem anderen Falle aber größer. Daraus

folgt aber ein wesentlicher Unterschied zwischen dem früher behandelten speziellen Falle und den jetzigen allgemeinen Erörterungen. Die elementaren symmetrischen Formen einer Größenreihe waren von einander unabhängig (Kap. II. § 15). Jetzt sind sie durch algebraische Relationen verknüpft, und die Anzahl der voneinander unabhängigen kann nicht größer als mn sein (Kap. V. § 15 u. 18). Sie ist sogar gleich mn, denn es gilt der Satz*):

Unter den elementaren symmetrischen Formen gibt es genau mn voneinander unabhängige Formen.

Der Beweis wird am einfachsten so geführt, daß wir eine solche Reihe unabhängiger Formen wirklich geben. Es sind dies die elementaren symmetrischen Formen (im früheren einfacheren Sinne des Wortes) der Reihen

$$x_{i1}, x_{i2}, \ldots, x_{in} \qquad (i = 1, \ldots, m),$$

die mit

$$\mathfrak{x}_r^{(i)} = \sum x_{ik_1} x_{ik_2} \ldots x_{ik_r}$$

bezeichnet werden mögen. Dann ist die Funktionaldeterminante

$$\frac{\partial(\ldots, \mathfrak{x}_r^{(i)}, \ldots)}{\partial(\ldots, x_{ir}, \ldots)}$$

geradezu gleich dem Produkte der m Funktionaldeterminanten

$$\frac{\partial(\mathfrak{x}_1^{(i)}, \ldots, \mathfrak{x}_n^{(i)})}{\partial(x_{i1}, \ldots, x_{in})}. \qquad (i = 1, \ldots, m)$$

Dieses ist (nach Kap. II. § 15) nichts anderes als

$$\prod_{r,s}(x_{ir} - x_{is}) \quad (r, s = 1, \ldots, n; r < s),$$

und demnach in der Tat von Null verschieden, womit der Satz bewiesen.

§ 19. Ohne die hier anknüpfenden allgemeinen Theorien weiter zu entwickeln, gehn wir unmittelbar auf den folgenden, für unsre Anwendungen wichtigen Hauptsatz über: .

*) Fr. Junker, Math. Annalen, 38. Bd., pag. 91.

Jede rationale, in Bezug auf die n Systeme $x_{1j}, \ldots, x_{mj}$ symmetrische Form ist als rationale Form der elementaren symmetrischen Formen darstellbar.

Man sieht unmittelbar, daß es genügt, den Satz für Typen zu beweisen. Wir unterscheiden nun die Typen nach der Anzahl der in den einzelnen Gliedern auftretenden verschiedenen Systeme und führen den Beweis zuerst für solche („einförmige“) Typen, in denen jedes einzelne Glied nur Unbestimmte eines Systems enthält.

Setzt man

$$T_j = \sum_{i=1}^{m} t_i x_{ij} \qquad (j = 1, \ldots, n),$$

wo $t_1, \ldots, t_n$ neue Unbestimmte bedeuten, so werden die elementaren symmetrischen Formen der n Größen T_j ihrer direkten Bildung nach homogene Formen der t, deren Koeffizienten geradezu elementare symmetrische Formen der Größensysteme $x_{1j}, \ldots, x_{mj}$ sind, und es ist demnach auch

$$\sum_{j=1}^{n} T_j^a$$

eine homogene Form der t, deren Koeffizienten sich rational und ganz aus jenen elementaren symmetrischen Formen zusammensetzen. Um also die Type

$$T^{(1)} = \sum x_{1j}^{a_1} x_{2j}^{a_2} \ldots x_{mj}^{a_m}$$

zu erhalten, hat man nur $a = a_1 + \cdots + a_m$ zu setzen und in der Darstellung von

$$\sum_{j=1}^{n} T_j^a = \sum_{j=1}^{n} (t_1 x_{1j} + t_2 x_{2j} + \cdots + t_m x_{mj})^a$$

den Koeffizienten von $t_1^{a_1} \ldots t_m^{a_m}$ zu bestimmen, der sich einerseits als das Produkt aus einem Polynomialkoeffizienten und $T^{(1)}$, andrerseits als rationale und ganze Form jener elementaren symmetrischen Formen ergibt.

Wenn wir annehmen, daß diese Darstellungsmethode für solche Typen schon erledigt ist, deren Glieder sich aus $k-1$ oder weniger verschiedenen Systemen zusammensetzen, so können wir eine ebensolche auch für diejenigen („k-förmigen") Typen festsetzen, deren Glieder Unbestimmte von k verschiedenen Systemen enthalten. Ist nämlich

$$T^{(k)} = \sum x_{1j_1}^{a_{11}} \dots x_{mj_1}^{a_{m1}} x_{1j_2}^{a_{12}} \dots x_{mj_2}^{a_{m2}} \dots x_{1j_k}^{a_{1k}} \dots x_{mj_k}^{a_{mk}}$$

eine solche Type, so wird das Produkt der beiden Typen

$$T^{(1)} = \sum x_{1j_1}^{a_{11}} \dots x_{mj_1}^{a_{m1}}, \quad T^{(k-1)} = \sum x_{1j_2}^{a_{12}} \dots x_{mj_2}^{a_{m2}} \dots x_{1j_k}^{a_{1k}} \dots x_{mj_k}^{a_{mk}}$$

sich gewiß als rationale Form der elementaren symmetrischen Formen darstellen lassen. Andrerseits gibt die Ausführung der Multiplikation die Type $T^{(k)}$ multipliziert mit einer rationalen und ganzen Zahl, wenn wir alle Glieder nehmen, in denen j_1 von $j_2, \dots, j_k$ verschieden ist. Alle andern Glieder des Produkts enthalten höchstens $k-1$ Systemen angehörige Unbestimmte und können daher in höchstens $k-1$-förmige Typen zusammengefaßt werden; damit ist die geforderte Darstellung von $T^{(k)}$ wirklich gefunden.

§ 20. Es sei

$$F_i(x_1, \dots, x_m) = 0 \qquad (i = 1, \dots, m) \tag{1}$$

ein „allgemeines" Gleichungssystem, d. h. ein solches, in dem F_i eine „allgemeine" Form n_i^{ter} Dimension bedeutet. Dasselbe besitzt demnach $N = n_1 \dots n_m$ Wurzelsysteme

$$\xi_{1j}, \xi_{2j}, \dots, \xi_{mj} \qquad (j = 1, \dots, N),$$

wo die Größen ξ als algebraische Funktionen der Koeffizienten $a_g^{(i)}$ zu fassen sind.

Indem man die Eliminante nach § 15 dieses Kapitels bildet, erhält man die Gleichung

$$R_{m+1} z^N + R_{m+1}^{(1)} z^{N-1} + \dots + R_{m+1}^{(N)} = 0, \tag{2}$$

deren Wurzeln die N linearen Formen

$$\sum_{i=1}^{m} t_i \xi_{ij} \qquad (j = 1, \ldots, N) \qquad (3)$$

sind. Dabei ist

$$R_{m+1} = \text{Res.} \begin{pmatrix} \varphi_1, \ldots, \varphi_m \\ x_1, \ldots, x_m \end{pmatrix} = r_0,$$

wo φ_i die Glieder n_i^{ter} Dimension in F_i bedeutet, R_{m+1} also eine rationale und ganze, irreduzible Form der Koeffizienten von $\varphi_1, \ldots, \varphi_m$ bedeutet. Ferner sieht man aus den früher entwickelten Eigenschaften der Resultante unmittelbar, daß $R_{m+1}^{(p)}$ eine homogene Form p^{ter} Dimension der t ist, deren Koeffizienten wieder rationale und ganze, homogene Formen der Koeffizienten $a_g^{(i)}$ werden, und zwar von der Dimension N_i in Bezug auf $a_g^{(i)}$, also von der Dimension $\sum_{i=1}^{m} N_i$ in Bezug auf alle a.

Demgemäß schreiben wir

$$R_{m+1}^{(p)} = r_{p1} T_1 + r_{p2} T_2 + \cdots,$$

wo die T die verschiedenen Potenzprodukte p^{ter} Dimension der t sind. Entsprechend sei auch

$$R_{m+1} = r_0 .$$

Bildet man nun die elementaren symmetrischen Formen der Wurzeln (3), die in gewohnter Weise mit

$$\mathfrak{f}_1, \mathfrak{f}_2, \ldots, \mathfrak{f}_N$$

bezeichnet werden mögen, so sieht man unmittelbar, daß diese homogene Formen der t sind, deren Koeffizienten geradezu elementare symmetrische Formen der Größensysteme $\xi_{1j}, \ldots, \xi_{mj}$ sind. Diese in irgend einer Reihenfolge mögen mit

$$\mathfrak{E}_1, \mathfrak{E}_2, \ldots, \mathfrak{E}_\mu$$

bezeichnet werden, und zwar tritt jedes $\mathfrak{E}$ als Koeffizient auf, so z. B.

$$\sum \xi_{r_1 j_1} \xi_{r_2 j_2} \cdots \xi_{r_k j_k}$$

als Koeffizient von $t_{r_1} t_{r_2} \ldots t_{r_k}$ in $\mathfrak{f}_k$. Andrerseits ist

$$r_0 \mathfrak{f}_k = (-1)^k R_{m+1}^{(k)} .$$

Vergleicht man also die Koeffizienten der verschiedenen Potenzprodukte, so erhält man die gesamten elementaren symmetrischen Formen der Größensysteme $\xi_{ij}, \ldots, \xi_{mj}$ geradezu gleich den Größen $(-1)^k \frac{r_{kl}}{r_0}$ und daraus sofort den allgemeinen Satz:

Jede rationale symmetrische Form der Größensysteme $\xi_{ij}, \cdots, \xi_{mj}$ ist als rationale Form der Größen $\frac{r_{kl}}{r_0}$ darstellbar, wo sämtliche r rationale und ganze Formen der $a_g^{(i)}$ sind.

Die für irgend eine symmetrische Form sich nach diesem Satze ergebende Relation

$$S(\cdots, \xi_{ij}, \cdots) = \sum_{(g)} C_g \left(\frac{r_{k_1 l_1}}{r_0}\right)^{g_1} \left(\frac{r_{k_2 l_2}}{r_0}\right)^{g_2} \cdots \qquad (S)$$

ist dabei so zu verstehen, daß, wenn rechts für jede der Größen $\frac{r_{kl}}{r_0}$ die entsprechende elementare symmetrische Form gesetzt wird, eine Identität entsteht, die auch dann richtig bleibt, wenn die ξ_{ij} beliebige unbestimmte Größen bedeuten.

Bei dieser Substitution entsteht aber rechts ein Ausdruck, der in den Größen eines Systems $\xi_{1j}, \ldots, \xi_{mj}$ höchstens zur Dimension d' ansteigt, wenn die rechts stehende Form in den $\frac{r_{kl}}{r_0}$ von der d'^{ten} Dimension ist.

Ist demnach die symmetrische Form S in Bezug auf irgend ein Größensystem $\xi_{ij}, \ldots, \xi_{mj}$ (also auch in Bezug auf jedes solche Größensystem) von der Dimension d, so ist $r_0^d S$ als rationale homogene Form der r_{kl} und r_0 darstellbar.

Denn die Dimension der rechts stehenden Form in (S) ist für irgend ein System $\xi_{1j}, \ldots, \xi_{mj}$, wie wir soeben gesehn kleiner oder gleich d'. Wäre nun in der Tat $d' > d$, so müßte, wenn man in S rechts für die $\frac{r_{kl}}{r_0}$ die entsprechenden elementaren symmetrischen Formen einsetzt, die Summe aller jener Glieder, deren Dimension $d+1, d+2, \cdots$ ist, für sich

verschwinden, was wegen der nun zwischen den $\mathfrak{E}$ bestehenden algebraischen Relationen ganz gut der Fall sein kann, und man erhält also die zweite Darstellung

$$S(\cdots, \xi_{ij}, \cdots) = \sum_{(h)} C_h \left(\frac{r_{k_1 l_1}}{r_0}\right)^{h_1} \left(\frac{r_{k_2 l_2}}{r_0}\right)^{h_2} \cdots,$$

wo die Form rechts nur mehr von der d^{ten} Dimension ist und also den ausgesprochenen Satz ergibt.

Dabei kann aber, wenn man unter den ξ_{ij} nicht mehr Unbestimmte, sondern ausschließlich Wurzelsysteme des Systems (1) versteht, — im Gegensatze zum speziellen Falle $m = 1$ — auch für eine kleinere Potenz von r_0 als die d^{te} schon $r_0^a S$ eine rationale und homogene Form der r_{kl} und r_0 werden. Für zwei Formen S und S', die in Bezug auf die einzelnen Größensysteme $\xi_{1j}, \ldots, \xi_{mj}$ von verschiedener Dimension sind, kann eben wegen der zwischen solchen Wurzelsystemen bestehenden algebraischen Relationen*) ganz gut $S = S'$ sein.

Als sofort zu verwendendes Beispiel einer symmetrischen Form bilden wir

$$\prod_{j=1}^{N} J(\xi_{1j}, \ldots, \xi_{mj}),$$

wo

$$J = \left| \frac{\partial F_i}{\partial x_j} \right|_{(i,j=1,\cdots,m)}$$

die Funktionaldeterminante des Formensystems $F_1, \ldots, F_m$ bezeichnet. J ist in den $x_1, \ldots, x_m$ von der Dimension

$$\sum_{i=1}^{m} n_i - m,$$

also

$$r_0^{\Sigma n_i - m} \prod_{j=1}^{N} J(\xi_{1j}, \ldots, \xi_{mj})$$

als homogene Form der $\Sigma n_i - m^{\text{ten}}$ Dimension in den r_{kl} und

*) Solche Relationen sind aus der Geometrie bekannt; z. B. der Schnittpunktsatz für zwei Curven dritter Ordnung.

r_0 darstellbar. Da aber die r_{kl} und r_0, sowie J wieder rationale und homogene Formen N_i^{ter}, resp. erster Dimension in Bezug auf die Koeffizientenreihe $a_y^{(i)}$ sind, so ist die so definierte Form von der Dimension $N_i\left(\sum_{i=1}^{m} n_i - m\right) + N$ in Bezug auf die Koeffizientenreihe $a_y^{(i)}$ und von der Dimension

$$\sum_{i=1}^{m} N_i\left(\sum_{i=1}^{m} n_i - m\right) + mN$$

in Bezug auf sämtliche Koeffizienten a.

Dementsprechend behält auch allgemein $r_0^d S(\ldots, \xi_{ij}, \ldots)$ für jedes spezielle System von Formen $F_1, \ldots, F_m$, wenn nur deren Dimension $n_1, \ldots, n_m$ sich nicht erniedrigt, seine Bedeutung als symbolische Definition gewisser aus den speziellen Koeffizienten der F zu bildender Größen, wenn nämlich festgesetzt wird, daß zuerst die Umrechnung auf eine Form der a und dann die Substitution jener speziellen Werte stattfindet. Es ist dies augenscheinlich eine Verallgemeinerung der in Kap. III. § 23 eingeführten symbolischen Darstellungen.

§ 21. Für den in dem vorstehenden Beispiele behandelten Ausdruck hat man nach § 17 unmittelbar

$$r_0^{\Sigma n_i - m} \prod_{j=1}^{N} J(\xi_{1j}, \ldots, \xi_{mj}) = \text{Res.}\begin{pmatrix} F_1, \ldots, F_m, J \\ x_1, \ldots, x_m, 1 \end{pmatrix}$$

in allen Fällen, wo die Definition der Resultante nicht ihren Sinn verliert. Da durchweg $n_i \geqq 1$ angenommen ist, kann dies nur dann geschehn, wenn die Dimension der Funktionaldeterminante gleich Null wird. Dies geschieht dann und nur dann, wenn sämtliche Formen linear sind. Sollte dies für allgemeine Formen auch sonst geschehn, so müßte dasselbe im speziellen Falle $F_i = x_i^{n_i}$ stattfinden; da aber die Funktionaldeterminante

$$N x_1^{n_1 - 1} \ldots x_m^{n_m - 1}$$

von der Dimension $\Sigma n_i - m$ und nicht Null wird, ist unsre

Behauptung erwiesen. Für den Ausnahmefall eines Systems linearer Formen wird, wie man unmittelbar sieht, jene symmetrische Form $= J = r_0$.

Man erkennt aber auch leicht, daß jener Ausdruck, als rationale Form der $a_y^{(i)}$ dargestellt, durch r_0 teilbar ist. Für den Ausnahmefall linearer Formen ist das evident; hat man es aber mit einer wirklichen Resultante zu tun, so muß diese bei solchen Werten der a, für die $r_0 = 0$ ist, verschwinden. Ist nämlich wieder φ_i der Komplex der Glieder höchster Dimension in F_i, so haben jetzt — dies ist eben die Bedeutung des Verschwindens von r_0 — die Gleichungen $\varphi_i = 0$ eine wirkliche Lösung. Der Komplex der Glieder höchster Dimension in J wird durch $\left|\frac{\partial \varphi_i}{\partial x_j}\right|$ gegeben. Da aber die φ homogene Formen sind, wird

$$x_h \left|\frac{\partial \varphi_i}{\partial x_j}\right| = A_{1h}\varphi_1 + \cdots + A_{mh}\varphi_m,$$

wenn man die h^{te} Spalte der Determinante mit x_h multipliziert und die mit $x_1, \ldots, x_m$ multiplizierten Elemente der ersten, $\ldots$, m^{ten} Spalte zu dieser addiert. Jene wirkliche Lösung der Gleichungen $\varphi_i = 0$ genügt also auch der Gleichung $\left|\frac{\partial \varphi_i}{\partial x_j}\right| = 0$; d. h. $F_1 = 0, \ldots, F_m = 0, J = 0$ haben eine im Unendlichen liegende wirkliche Lösung, und die Resultante muß Null sein für jedes Wertsystem der a, bei dem $r_0 = 0$ ist. Da nun r_0 irreduzibel und also $r_0 = 0$ eine irreduzible Mannigfaltigkeit ist, folgt hieraus nach den in Kap. V § 7 entwickelten Methoden, oder einfacher aus dem in der Fußnote zu § 15 d. Kap. gegebenen Hilfssatze, daß jene Resultante durch r_0 teilbar ist. Es ist demnach

$$\text{Res.}\begin{pmatrix} F_1, \ldots, F_m, J \\ x_1, \ldots, x_m, 1 \end{pmatrix} = r_0 D,$$

wo D eine rationale Form der $a_y^{(i)}$ ist, denn der Schluß auf die Teilbarkeit der Resultante durch r_0 bezieht sich selbstverständlich auf den Bereich der rationalen Zahlen (1). D muß aber eine rationale und ganze Form sein. Denn es ist jeden-

falls, wenn D' eine primitive rationale und ganze Form, p und q rationale und ganze Zahlen bedeuten,

$$D = \frac{p}{q} D'.$$

Da aber r_0 eine irreduzible rationale und ganze Form ist, muß in der Tat p durch q teilbar sein.

Man hat daher das auch für ein System linearer Formen gültige Resultat, daß

$$r_0^{\Sigma n_i - m - 1} \prod_{j=1}^{N} J(\xi_{1j}, \ldots, \xi_{mj})$$

eine rationale und ganze Form der $a_y^{(i)}$ ist, die man Discriminante des Formensystems $F_1, F_2, \ldots, F_m$ nennt, und mit Dscr. $(F_1, \ldots, F_m)$ oder notwendigen Falls mit Dscr. $\begin{pmatrix} F_1, \ldots, F_m \\ x_1, \ldots, x_m \end{pmatrix}$ bezeichnet. Wir behalten diese Benennung auch dann bei, wenn die Koeffizienten $a_y^{(i)}$ irgend welche Werte annehmen, was so zu verstehen ist, daß diese speziellen Werte erst in dem fertigen Ausdruck der Discriminante als rationaler und ganzer Form der $a_y^{(i)}$ zu substituieren sind.

Die Irreduzibilität der Funktionaldeterminante.

§ 22. Wir schalten hier den Beweis eines im folgenden wichtigen Hilfssatzes ein:

Die Funktionaldeterminante J eines allgemeinen Formensystems $F_i(x_1, \ldots, x_m)$, $(i = 1, \ldots, m)$, wo $n_i \geq 1$, ist, als rationale und ganze Form der a und x aufgefaßt, irreduzibel.

Für den Fall linearer Formen:

$$L_i = \sum_{j=1}^{m} c_{ij} x_j, \qquad (i = 1, \ldots, m)$$

ist die Funktionaldeterminante $| c_{ij} |_{(i,j=1, \ldots, m)}$; sie enthält die x überhaupt nicht. Daß diese Determinante eine irreduzible Form der c darstellt, wurde schon im § 11 dieses Kapitels bewiesen.

Indem wir auf den Fall übergehen, wo nicht alle Formen linear sind, können wir den Komplex der linearen Glieder von F_i mit L_i bezeichnen; es ist dann wieder

$$L_i = \sum_{j=1}^{m} c_{ij} x_j \qquad (i = 1, \ldots, m)$$

und

$$J = |c_{ij}| + C_1 X_1 + C_2 X_2 + \cdots,$$

wo $X_1, X_2, \ldots$ von 1 verschiedene Potenzprodukte der x bezeichnen.

Jeder echte Teiler von J muß, wie J selbst, homogen in Bezug auf jede Reihe $a_y^{(i)}$ sein und wird — wieder mit J — in Bezug auf eine solche Reihe entweder linear sein, oder diese gar nicht enthalten. Es muß endlich dieser Teiler die Gestalt

$$d = A_0 + A_1 X_1 + A_2 X_2 + \cdots$$

haben, und A_0, das von den x freie Glied, von 0 verschieden sein, da sonst $|c_{ij}| = 0$ folgen würde. Der komplementäre Teiler wäre dann:

$$d' = A'_0 + A'_1 X_1 + A'_2 X_2 + \cdots$$

und demnach

$$A_0 A'_0 = |c_{ij}|;$$

es ist also entweder A_0 oder A'_0 gleich ± 1; und da d und d' in jeder Reihe $a_y^{(i)}$, die sie enthalten, homogen und linear sind, hat einer dieser beiden echten Teiler, neben den Potenzprodukten X, Koeffizienten, die durchweg rationale und ganze Zahlen sind.

Ein solcher Teiler von J müßte demnach auch dann ein Teiler von J bleiben, wenn man die $a_y^{(i)}$ irgendwie als ganze Zahlen annimmt. Man kann also z. B wieder $F_i = L_i$ setzen, und es müßte also jener echte Teiler auch ein Teiler von $|c_{ij}|$ sein, d. h. auch die x nicht enthalten; demnach hat J in der Tat nur die Teiler ± 1, $\pm J$.

Mit den in § 11 und hier dargelegten Methoden zeigt man auch, daß die Funktionaldeterminante eines allgemeinen Formensystems, in welchem die Dimension jeder Form $\geqq 1$ ist, als Form der a und x aufgefaßt, im Sinne von Kap. IV § 18 absolut irreduzibel ist.

Die Grundeigenschaften der Discriminante.

§ 23. Ist wieder $F_1, \ldots, F_m$ ein allgemeines Formensystem ($n_i \geqq 1$) und J dessen Funktionaldeterminante, so wird nach § 17 und 21

$$\text{Res.}\begin{pmatrix} F_1, \ldots, F_m, J \\ x_1, \ldots, x_m, 1 \end{pmatrix} = r_0^{\Sigma n_i - m} \prod_{k=1}^{N} J(\xi_{1k}, \ldots, \xi_{mk})$$

$$\text{Dscr.}\begin{pmatrix} F_1, \ldots, F_m \\ x_1, \ldots, x_m \end{pmatrix} = r_0^{\Sigma n_i - m - 1} \prod_{k=1}^{N} J(\xi_{1k}, \ldots, \xi_{mk})$$

und daher, wenn wir die Discriminante des Formensystems kurz mit D bezeichnen, auch

$$\text{Res.}\begin{pmatrix} F_1, \ldots, F_m, J \\ x_1, \ldots, x_m, 1 \end{pmatrix} = r_0 D.$$

Wir schließen von nun ab den Fall eines Systems von durchweg linearen Formen aus, setzen also $N > 1$, und beweisen dann, daß die in den vorhergehenden Erörterungen als rationale und ganze Form erkannte Discriminante dem durch das Modulsystem $(F_1, \ldots, F_m, J)$ definierten Kongruenzbereiche angehört:

$$D \equiv 0 \ (\text{mod. } J, F_1, \ldots, F_m). \qquad \text{(I)}$$

Da diese Eigenschaft für die Resultante des Formensystems $J, F_1, \ldots, F_m$ feststeht, hat man jedenfalls

$$r_0 D = K_0 J + \sum_{i=1}^{m} K_i F_i.$$

Wenn man weiter in dieser Identität, wo $K_0, \ldots, K_m$ rationale und ganze Formen der a und x bedeuten, wieder

$$a_{i,m+1} - F_i \quad \text{statt} \quad a_{i,m+1} \qquad (i = 1, \ldots, m)$$

setzt, erhält man, da r_0 und J die Unbestimmten $a_{i,m+1}$ gar nicht enthalten:

$$r_0 [D] = [K_0] J,$$

wo das Zeichen [. . .], wie früher, die Ausführung dieser Substitution andeutet. Da aber r_0 die x nicht enthält, während J irreduzibel ist, so folgt hieraus, sobald J die Unbestimmten x enthält, daß $[D]$ durch J teilbar sein muß, und dies ist nur eine andere Ausdrucksweise für die Kongruenz (I).

Damit ist der ausgesprochene Satz bewiesen; denn die Funktionaldeterminante eines nicht durchweg aus linearen Formen bestehenden Systems enthält wenigstens eine der Unbestimmten. Um dies einzusehn, bemerke man nur, daß es auch dann noch der Fall ist, wenn man die Formen bei Erhaltung ihrer Dimension z. B. in folgender Weise spezialisiert:

$$x_1^{n_1},\ x_2^{n_2},\ \ldots,\ x_m^{n_m}.$$

Ist hier z. B. $n_i > 1$, so wird die Funktionaldeterminante

$$N \ldots x_i^{n_i - 1} \ldots$$

die Unbestimmte x_i sicher enthalten.

§ 24. Für die weiteren Entwicklungen ist es von Wichtigkeit, die Discriminante eines Systems von Formen, deren jede das Produkt allgemeiner linearer Formen ist, genauer zu kennen.

Dazu muß vor allem die Gestalt der Funktionaldeterminante in diesem Falle bestimmt werden. Man sieht unmittelbar, daß, wenn eine Form als Produkt dargestellt ist:

$$F_1 = F_1' F_1'',$$

für die Funktionaldeterminante

$$\frac{\partial(F_1' F_1'', F_2, \ldots, F_m)}{\partial(x_1, x_2, \ldots, x_m)} =$$

$$= F_1'' \frac{\partial(F_1', F_2, \ldots, F_m)}{\partial(x_1, x_2, \ldots, x_m)} + F_1' \frac{\partial(F_1'', F_2, \ldots, F_m)}{\partial(x_1, x_2, \ldots, x_m)}$$

folgt. Durch wiederholte Anwendung dieser Identität erhält man, wenn allgemein

$$F_i = L_{i1} \ldots L_{i\mu_i} \ldots L_{in_i} \qquad (i = 1, \ldots, m) \quad \text{(I)}$$

gesetzt wird:

$$\frac{\partial(F_1, \ldots, F_m)}{\partial(x_1, \ldots, x_m)} = \sum \frac{F_1 \ \ldots \ F_m}{L_{1\mu_1}, \ldots, L_{m\mu_m}} \frac{\partial(L_{1\mu_1}, \ldots, L_{m\mu_m})}{\partial(x_1, \ldots, x_m)},$$

wo die Summation sich auf alle Kombinationen $(1, \mu_1), \ldots, (m, \mu_m)$ erstreckt, in denen $\mu_1, \ldots, \mu_m$ voneinander unabhängig beliebige Zahlen der Reihen $(1, \ldots, n_1), \ldots, (1, \ldots, n_m)$ bedeuten. Setzt man nun, wie früher (§ 11):

$$L_{i\mu_i} = c_{i1}^{(\mu_i)} x_1 + \cdots + c_{im}^{(\mu_i)} x_m + c_{i,m+1}^{(\mu_i)},$$

so wird nach dem Produktsatz für Resultanten jetzt

$$r_0 = \prod_{\mu_m=1}^{n_m} \cdots \prod_{\mu_1=1}^{n_1} \left| c_{ij}^{(\mu_i)} \right|_{(i,j=1,\cdots,m)}$$

und für diejenige Wurzel des Systems $F_i = 0$, die dem linearen Systeme

$$L_{1\mu_1} = 0, \ L_{2\mu_2} = 0, \ \ldots, \ L_{m\mu_m} = 0$$

entspricht und die mit $\xi_{1\mu_1}, \ldots, \xi_{m\mu_m}$ bezeichnet werden soll, der Wert der Funktionaldeterminante

$$\left(\frac{F_1 \ \ldots \ F_m}{L_{1\mu_1} \ldots L_{m\mu_m}}\right)_{\xi_{1\mu_1}, \ldots, \xi_{m\mu_m}} \left| c_{ij}^{(\mu_i)} \right|,$$

wo der Quotient im ersten Faktor nur die Bedeutung hat, daß aus dem Produkte $F_1 \ldots F_m$ der Reihe nach $L_{1\mu_1}, \ldots, L_{m\mu_m}$ zu entfernen ist, und endlich für die Discriminante des in (I) definierten Formensystems:

$$r_0^{\Sigma n_i - m} \prod_{\mu_m=1}^{n_m} \cdots \prod_{\mu_1=1}^{n_1} \left(\frac{F_1 \ \ldots \ F_m}{L_{1\mu_1} \ldots L_{m\mu_m}}\right)_{\xi_{1\mu_1}, \ldots, \xi_{m\mu_m}}.$$

Nun sind $\xi_{1\mu_1}, \ldots, \xi_{m\mu_m}$ Quotienten zweier Formen, deren Nenner die Determinante $\left| c_{ij}^{(\mu_i)} \right|$ und deren Zähler eine ähnlich gebildete Determinante ist, wo nur an Stelle der Elemente der j^{ten} Spalte die Elemente $-c_{i,m+1}^{(\mu_i)}$ treten. Der unter dem Produktzeichen stehende allgemeine Faktor, der $\Sigma n_i - m$ lineare Faktoren enthält, wird also ganz, wenn man aus $r_0^{\Sigma n_i - m}$ gerade den Faktor $\left| c_{ij}^{(\mu_i)} \right|^{\Sigma n_i - m}$ zu diesem hinzunimmt. Die so ent-

stehenden Faktoren des Ausdrucks für Dscr. $(F_1, \ldots, F_m)$ haben demnach die Gestalt

$$c_{k1}^{(\nu_k)}\left\{\left|c_{ij}^{(\mu_i)}\right|\right\}_1 + \cdots + c_{km}^{(\nu_k)}\left\{\left|c_{ij}^{(\mu_i)}\right|\right\}_m + c_{k,m+1}^{(\nu_k)}\left|c_{ij}^{(\mu_i)}\right|,$$

wo $\left\{\left|c_{ij}^{(\mu_i)}\right|\right\}_r$ diejenige Determinante bezeichnet, die aus $\left|c_{ij}^{(\mu_i)}\right|$ entsteht, wenn in der r^{ten} Spalte an Stelle der Elemente $c_{1r}^{(\mu_1)}, \ldots, c_{mr}^{(\mu_m)}$ der Reihe nach $-c_{1,m+1}^{(\mu_1)}, \ldots, -c_{m,m+1}^{(\mu_m)}$ treten, und das Zahlenpaar k, ν_k nicht mit den Zahlenpaaren $1, \mu_1$; $2, \mu_2 \ldots$ oder m, μ_m übereinstimmen. Diese Faktoren, deren Anzahl $N(\Sigma n_i - m)$ ist, und in denen $c_{ij}^{(\mu_i)}$ durchweg verschiedene Unbestimmte bedeuten, sind demnach in Bezug auf die Unbestimmten $c_{k1}^{(\nu_k)}, \ldots, c_{k,m+1}^{(\nu_k)}$ immer linear und zwei derselben niemals äquivalent. Jeder solche Faktor wird durch die Zahlenpaare $(k, \nu_k), (1, \mu_1), \ldots, (m, \mu_m)$ vollständig bestimmt, und zwei verschiedene Faktoren, in denen diese Zahlenpaare eben nicht sämtlich übereinstimmen, enthalten auch verschiedene Unbestimmte. Es ist auch jeder solche Faktor irreduzibel, denn die Koeffizienten der linear auftretenden Unbestimmten $c_{k1}^{(\nu_k)}, \ldots, c_{k,m+1}^{(\nu_k)}$:

$$\left\{\left|c_{ij}^{(\mu_i)}\right|\right\}_1, \ldots, \left\{\left|c_{ij}^{(\mu_i)}\right|\right\}_m, c_{ij}^{(\mu_i)}$$

haben keinen gemeinschaftlichen Teiler. Daraus folgt endlich noch, daß keiner dieser Faktoren durch eine Determinante $\left|c_{ij}^{(\mu_i)}\right|$ teilbar sein kann, denn jener irreduzible Faktor hat die Dimension $m+1$ und demnach überhaupt keinen Teiler von der Dimension m.

Es ist demnach die Discriminante des in (I) gegebenen Formensystems nichts anderes als ein Resultantenprodukt*)

$$\Pi \text{Res.}\,(L_{1\mu_1}, L_{2\mu_2}, \ldots, L_{m\mu_m}, L_{k\nu_k}), \qquad \text{(II)}$$

wo das Produkt über alle Resultanten zu erstrecken ist, die

*) Jede einzelne Determinante ist — der früheren Darstellung gegenüber — mit dem Zeichen $(-1)^m$ genommen. Ihre Anzahl $N(\Sigma n_i - m)$ ist aber immer gerade.

man erhält, wenn man $\mu_i = 1, \ldots, n_i$ setzt, und jeder Kombination $(\mu_1, \ldots, \mu_m)$ der Reihe nach alle $L_{k\nu_k}$ hinzufügt, wo (k, ν_k) ein von $(1, \mu_1), \ldots, (m, \mu_m)$ verschiedenes Zahlenpaar ist.

Die Discriminante eines Formensystems, deren jede ein Produkt allgemeiner linearer Formen ist, ist daher ein Produkt von durchweg verschiedenen irreduzibeln Formen und durch r_0 nicht teilbar. (Dabei ist, wie mehrfach festgestellt, r_0 die Resultante jenes homogenen Formensystems, wo jede Form nur die Glieder höchster Dimension der ursprünglichen Formen enthält.)

§ 25. Wir gehn nun zu dem Beweise des fundamentalen Satzes über, daß die Discriminante eines allgemeinen Formensystems eine irreduzible rationale und ganze Form der Koeffizienten $a_g^{(i)}$ ist*).

Diese Discriminante D hat als rationale und ganze Form der $a_g^{(i)}$ jedenfalls die Gestalt

$$D = r_0^c P_1^{c_1} \ldots P_k^{c_k}.$$

Daß jedenfalls $c = 0$, $c_1 = \cdots = c_k = 1$ sein muß, folgt aus dem soeben erörterten speziellen Fall. Setzt man nämlich an Stelle der $a_g^{(i)}$ die für $F_i = L_{i1}, \ldots, L_{in_i}$ als Koeffizienten resultierenden homogenen Formen der $c_{ij}^{(\mu_i)}$, so wird D nicht Null, also auch $r_0, P_1, \ldots, P_k$ von Null verschieden sein; es wäre also, wenn die c nicht die erwähnten Werte annehmen, D durch r_0 teilbar, oder es würde D einen mehrfachen Faktor enthalten, was nach dem Vorstehenden unmöglich ist. Es muß also

$$D = P_1 \ldots P_k$$

sein. Man hat daher — anschließend an die Erörterungen des § 23 —

$$[P_1] \ldots [P_k] \equiv 0 \pmod{J}$$

*) Dieser Satz ist in der Kroneckerschen „Festschrift" (§ 10) beiläufig erwähnt, der Beweis für eine weitere, leider nie erschienene Abhandlung versprochen.

und, da die Funktionaldeterminante J irreduzibel ist, auch für ein P, es sei dies P_1:

$$[P_1] \equiv 0 \text{ (mod. } J)$$

oder:

$$P_1 \equiv 0 \text{ (mod. } F_1, \ldots, F_m, J).$$

Es mögen nun die $a_g^{(i)}$ irgend welche Werte annehmen, für welche P_r Null wird. Dann wird für dieses Wertsystem r_0 entweder auch verschwinden oder nicht. Im letzteren Falle verschwindet Res. $(F_1, \ldots, F_m, J)$, ohne daß r_0 Null ist; die Gleichungen $F_1 = 0, \ldots, F_m = 0, J = 0$ besitzen daher eine gemeinschaftliche endliche Lösung. Setzt man diese für $x_1, \ldots, x_m$ in $F_1, \ldots, F_m, J$ ein, so folgt aus der letzten Kongruenz, daß für dasselbe Wertsystem der $a_g^{(i)}$ auch P_1 verschwindet. Alles zusammengenommen, sieht man also, daß für jedes Wertsystem der $a_g^{(i)}$, für welches P_r verschwindet, entweder r_0 oder P_1 Null sein muß, also $r_0 P_1$ auch verschwindet; es muß also nach dem in der Fußnote zu § 15 d. Kap. gegebenen einfachen Hilfssatze, $r_0 P_1$ durch P_r teilbar sein, was aber nicht möglich ist, da r_0 und P_1 der Annahme nach von P_r verschiedene irreduzible Formen bedeuten. Folglich kann D neben P_1 keinen zweiten irreduzibeln Teiler enthalten, und es ist $D \sim P_1$, w. z. b. w.

§ 26. Es seien die den allgemeinen Formen $F_i(x_1, \ldots, x_m)$, wo wieder $N > 1$ angenommen ist, entsprechenden homogenen Formen wieder $\Phi_i(x_1, \ldots, x_{m+1})$ und wie früher

$$F_i^{(k)} = (\Phi_i(x_1, \ldots, x_{m+1}))_{x_k=1},$$

also $F_i^{(m+1)} = F_i$, ferner, den bisherigen Bezeichnungen entsprechend:

$$\varphi_i^{(k)} = (\Phi_i(x_1, \ldots, x_{m+1}))_{x_k=0}$$

und noch

$$\varrho_k = \text{Res.} \left(\varphi_1^{(k)}, \ldots, \varphi_m^{(k)}\right),$$

also $\varphi_i^{(m+1)}$ jene homogene Form, die bisher mit φ_i bezeichnet wurde, und ϱ_{m+1} das bisherige r_0. Man sieht un-

mittelbar, daß $\varrho_1, \ldots, \varrho_{m+1}$ durchweg verschiedene irreduzible Formen sind.

Bedeutet D die im Vorhergehenden definierte Discriminante des Formensystems $F_1, \ldots, F_m$ und $a_g^{(i)} = \alpha_g^{(i)}$ irgend ein Wertsystem, für welches D verschwindet, $\varrho_1, \ldots, \varrho_{m+1}$ aber von Null verschieden sind, so besitzen bei dieser Spezialisation auch die Gleichungen $F_i = 0$ ein endliches Wurzelsystem, das der Gleichung

$$|F_{ij}| = 0 \qquad (i, j = 1, \ldots, m)$$

genügt; und zwar wird, wenn man dieses Wurzelsystem mit $\xi_1, \ldots, \xi_m$ bezeichnet, infolge der Bedingung $\varrho_k \neq 0$ keine der Größen ξ gleich Null sein.

Es sei jetzt $H^{(k)}$ die Funktionaldeterminante von $\Phi_1, \ldots, \Phi_m$ nach $x_1, \ldots, x_{m+1}$ mit Ausschluß von x_k; dann ist das Gleichungssystem

$$\Phi_1 = 0, \ldots, \Phi_m = 0, H^{(k)} = 0 \qquad (\Sigma_k)$$

nichts anderes, als das durch Einführung der Unbestimmten x_k homogen gewordene System:

$$F_1^{(k)} = 0, \ldots, F_m^{(k)} = 0, J^{(k)} = 0,$$

wo

$$J^{(k)} = \left| F_{ij}^{(k)} \right|_{(i=1,\ldots,m;\, j=1,\ldots,m+1;\, j \neq k)}.$$

Zwischen den Funktionaldeterminanten $H^{(k)}$ besteht die Relation:

$$x_{m+1} H^{(k)} \equiv \pm x_k H^{(m+1)} \pmod{\Phi_1, \ldots, \Phi_m},$$

wie man leicht sieht, wenn man in $H^{(k)}$, $(k \neq m+1)$ die letzte Spalte mit x_{m+1} multipliziert, dann die der Reihe nach mit $x_1, \ldots, x_m$ (mit Ausschluß von x_k) multiplizierten Elemente der übrigen Spalten zu den Elementen der letzten Spalte addiert und endlich die Identität

$$\sum_{j=1}^{m+1}{}^{(k)} x_j \Phi_{ij} = - x_k \Phi_{ik} + n_i \Phi_i$$

berücksichtigt.

Ist demnach $\alpha_y^{(i)}$ ein den oben angegebenen Bedingungen gemäß gewähltes Koeffizientensystem, so wird, wenn $\xi_1, \ldots, \xi_m$ die früher festgesetzten Größen sind und $\xi_{m+1} = 1$ ist, das Größensystem $\xi_1, \ldots, \xi_{m+1}$ ein wirkliches Wurzelsystem jedes Gleichungssystems (Σ_k) sein, und es ist auch

$$\frac{\xi_j}{\xi_k}, \quad (j = 1, \ldots, m+1; j \neq k)$$

eine wirkliche Lösung des Gleichungssystems

$$F_1^{(k)} = 0, \ldots, F_m^{(k)} = 0, J^{(k)} = 0.$$

Es ist also bei diesen Annahmen auch die Discriminante des Systems $F_i^{(k)}$, die wir mit $D^{(k)}$ bezeichnen können, gleich Null.

Für jedes Wertsystem $a_y^{(i)}$, welches $D = 0$ nach sich zieht, wird demgemäß entweder ein ϱ Null, oder $D^{(k)} = 0$, also $\varrho_1 \varrho_2 \ldots \varrho_{m+1} D^{(k)}$ gewiß gleich Null. Diese Größe wird infolgedessen (nach dem Hilfssatze in § 15) durch D teilbar sein. Nun ist D irreduzibel, und kein ϱ kann durch D teilbar sein, wie dies nach der Untersuchung des Falles, wo die F Produkte linearer Formen sind, unmittelbar klar ist, denn die irreduzibeln Faktoren von ϱ sind dann von der m^{ten}, die von D von der $m+1^{\text{ten}}$ Dimension; es muß also $D^{(k)}$ durch D teilbar sein, mithin können sich diese beiden irreduzibeln Formen nur im Vorzeichen unterscheiden; oder allgemeiner ausgesprochen:

Die Discriminanten $D^{(1)}, D^{(2)}, \ldots, D^{(m+1)} = D$ können sich nur im Vorzeichen unterscheiden.

Das Wurzelsystem $\xi_1, \ldots, \xi_{m+1}$ entspricht nun auch dem Systeme:

$$\Phi_1 = 0, \ldots, \Phi_m = 0, \sum_{k=1}^{m+1} t_k J^{(k)} = 0,$$

wo $t_1, \ldots, t_{m+1}$ neue Unbestimmte bedeuten, und die Resultante dieses Systems verschwindet für jedes wie früher charakterisierte Wertsystem $a_y^{(i)}$, d. h. jene Resultante ist eine homogene Form der t, ausführlicher geschrieben:

$$\sum A_g t_1^{g_1} \dots t_{m+1}^{g_{m+1}} \quad (g_1 + \dots + g_{m+1} = N),$$

wo auch jeder einzelne Koeffizient diese Eigenschaft besitzt. Demnach wird $\varrho_1 \dots \varrho_{m+1} A_g$ durch D teilbar, und da kein ϱ durch D teilbar ist, muß jedes A_g durch D teilbar sein. Man sieht aber leicht, daß D der größte gemeinschaftliche Teiler der Koeffizienten A_g ist. Man erhält nämlich den Koeffizienten von t_k^N wenn man jedes t, mit Ausschluß von t_k, gleich 0 und $t_k = 1$ setzt; dann wird aber jene Resultante die Resultante von $\Phi_1, \Phi_2, \dots, \Phi_m, H^{(k)}$ oder auch die Resultante von

$$F_1^{(k)}, F_2^{(k)}, \dots, F_m^{(k)}, J^{(k)},$$

d. h. $\varrho_k D$; da aber $\varrho_1, \dots, \varrho_{m+1}$ teilerfremd sind, ist der gemeinschaftliche Teiler D auch der größte gemeinschaftliche Teiler jener Koeffizienten A.

Wir wollen — ebenso wie bei der Resultante — unter der Discriminante der m homogenen Formen $\Phi_1, \dots, \Phi_m$ geradezu die Discriminante von $F_1, \dots, F_m$ verstehn; dabei ist selbstverständlich eine bestimmte Anordnung der Unbestimmten x ins Auge gefaßt; ist eine solche nicht gegeben, so bleibt das Vorzeichen der Discriminante unbestimmt, was aber ihrer jetzigen Definition als größten gemeinschaftlichen Teilers naturgemäß entspricht.

Man gelangt damit zu folgender, von Kronecker*) herrührenden Definition der Discriminante eines homogenen Formensystems, die zugleich eine wichtige Eigenschaft der Discriminante ausdrückt:

Sind $\Phi_i(x_1, \dots, x_{m+1})$, $(i = 1, \dots, m)$ allgemeine homogene Formen der Dimension $n_1, \dots, n_m$, $(N > 1)$ und bedeutet Φ_{m+1} eine allgemeine homogene lineare Form

*) Festschrift, § 10. Der an dieser Stelle gegebene allgemeinere Satz für eine Form Φ_{m+1}, deren Dimension n_{m+1} ist, ist, wie die weiteren Ausführungen des Textes zeigen, dahin richtig zu stellen, daß der von den Koeffizienten der Form Φ_{m+1} unabhängige Faktor jener Resultante nicht Dscr. $(\Phi_1, \dots, \Phi_m)$, sondern n_{m+1}^N Dscr. $(\Phi_1, \dots, \Phi_m)$ ist.

mit neuen unbestimmten Koeffizienten, so hat die Resultante der Formen

$$\Phi_1, \ldots, \Phi_m, \; |\Phi_{ij}|_{(i,j=1,\cdots,m+1)}$$

einen von den Koeffizienten der Form Φ_{m+1} unabhängigen Faktor, und dieser ist nichts anderes, als die Discriminante des Formensystems $\Phi_1, \ldots, \Phi_m$.

Man sieht unmittelbar, daß für

$$\Phi_{m+1} = \sum_{k=1}^{m+1} t_k x_k \quad \text{nun} \quad \sum_{k=1}^{m+1} t_k H^{(k)} = |\Phi_{ij}| \text{ ist.}$$

Dieser Satz kann noch allgemeiner und genauer gefaßt werden:

Ist Φ_{m+1} eine allgemeine homogene Form der Dimension n_{m+1} mit neuen unbestimmten Koeffizienten, so wird die Resultante der Formen

$$\Phi_1, \ldots, \Phi_m, \; |\Phi_{ij}|_{(i,j=1,\cdots,m+1)}$$

gleich

$$n_{m+1}^N \operatorname{Res.}(\Phi_1, \ldots, \Phi_{m+1}) \operatorname{Dscr.}(\Phi_1, \ldots, \Phi_m).$$

Um das einzusehn, berücksichtige man, daß

$$\operatorname{Res.}(\Phi_1, \ldots, \Phi_m, x_{m+1}) = \varrho_{m+1},$$

und benutze den für die Resultante entwickelten Produktsatz. Bezeichnet man die zu bestimmende Resultante mit R, so wird:

$$\varrho_{m+1} R = \operatorname{Res.}(\Phi_1, \ldots, \Phi_m, x_{m+1} \, |\Phi_{ij}|);$$

oder also nach Umformung von $x_{m+1} \, |\Phi_{ij}|$ auch

$$\varrho_{m+1} R = \operatorname{Res.}\left(\Phi_1, \ldots, \Phi_m, \sum_{k=1}^{m+1} n_k \Phi_k H_k\right)$$

$$= \operatorname{Res.}\left(F_1, \ldots, F_m, \sum_{k=1}^{m+1} n_k F_k J_k\right),$$

wo H_k, bez. J_k die Funktionaldeterminante der Φ_i, bez. F_i, $(i = 1, \ldots, m+1; \, i \neq k)$ nach $x_1, \ldots, x_m$ bedeutet. Weiter wird, wenn man die Poissonsche Gestalt der Resultante benutzt:

$$R = \varrho_{m+1}^{\Sigma n_j - m} \prod_{k=1}^{N} n_k F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}) J(\xi_{1k}, \ldots, \xi_{mk})$$

$$= n_{m+1}^{N} \varrho_{m+1}^{n_{m+1}} \prod_{k=1}^{N} F_{m+1}(\xi_{1k}, \ldots, \xi_{mk}) \varrho_{m+1}^{\Sigma n_i - m - 1} \prod_{k=1}^{N} J(\xi_{1k}, \ldots, \xi_{mk}),$$

und dies ist nichts anderes, als die in unserem Satze behauptete Gestalt der Resultante.

Die Invarianteneigenschaft der Discriminante.

§ 27. Die soeben erhaltene neue Definition der Discriminante ergibt auch den folgenden Satz, in dem sämtliche Bezeichnungen des vorigen § beibehalten sind.

Das Verschwinden der Discriminante des Formensystems $\Phi_1, \ldots, \Phi_m$, wo $N > 1$ ist, ist die notwendige und hinreichende Bedingung für die Existenz einer solchen wirklichen Lösung des Gleichungssystems

$$\Phi_1 = 0, \ldots, \Phi_m = 0, \sum_{k=1}^{m+1} t_k H^{(k)} = 0, \qquad (\Sigma)$$

in welcher die in dem Wurzelsysteme auftretenden Größen von den t unabhängig sind. Dabei sind $t_1, \ldots, t_{m+1}$ wieder als Unbestimmte, $x_1, \ldots, x_{m+1}$ als Unbekannte aufzufassen.

Eine wirkliche Lösung existiert, wenn die Resultante

$$\sum A_g t_1^{g_1} \ldots t_{m+1}^{g_{m+1}}, \quad (g_1 + \cdots + g_{m+1} = N)$$

verschwindet, also, da die t Unbestimmte sind, wenn jeder Koeffizient A_g Null ist, d. h. wenn für die Koeffizienten $a_y^{(i)}$ der Formen Φ solche Wertsysteme gesetzt werden, die dem Gleichungssysteme $A_g = 0$ genügen.

Nun ist (§ 26) $A_g = DA'_g$, und also $D = 0$ eine jedenfalls hinreichende Bedingung. Ist nun umgekehrt $a_y^{(i)}$ ein Koeffizientensystem, das für die Gleichungen (Σ) ein von den t unabhängiges Wurzelsystem ergibt, so ist in diesem

ein x, z. B. x_k, gewiß nicht Null. Damit ergibt sich aber auch ein (endliches) Wurzelsystem der Gleichungen

$$F_1^{(k)} = 0, \ldots, F_m^{(k)} = 0, \; |F_{ij}^{(k)}| = 0.$$

Nun ist

$$D \equiv 0 \; (\text{mod. } F_1^{(k)}, \ldots, F_m^{(k)}, \; |F_{ij}^{(k)}|),$$

also, wenn man statt der x in die durch diese Kongruenz angedeutete Identität jenes Wurzelsystem einsetzt, für jenes Koeffizientensystem auch $D = 0$, womit der Satz bewiesen.

Dieser Satz enthält dem Wesen nach auch schon die s. g. Invarianteneigenschaft der Discriminante, was jetzt näher dargelegt werden soll.

Die Formen

$$\Phi_1, \ldots, \Phi_m, \; \Phi_{m+1} = \sum_{k=1}^{m+1} t_k x_k$$

mögen durch die lineare Transformation

$$x_j = \sum_{k=1}^{m+1} u_{jk} \bar{x}_k \qquad (T)$$

wieder nach der schon früher angewandten Bezeichnung in

$$\bar{\Phi}_1, \ldots, \bar{\Phi}_m, \; \bar{\Phi}_{m+1}$$

übergehn. Man hat dann

$$\frac{\partial \bar{\Phi}_i}{\partial \bar{x}_j} = \overline{\frac{\partial \Phi_i}{\partial x_1}} u_{1j} + \cdots + \overline{\frac{\partial \Phi_i}{\partial x_{m+1}}} u_{m+1,j},$$

wo $\overline{\frac{\partial \Phi_i}{\partial x_k}}$ in naturgemäßer Fortführung der gebrauchten Bezeichnung die durch Ausführung der Transformation (T) aus $\frac{\partial \Phi_i}{\partial x_k}$ erhaltene Form bedeutet. Demnach wird:

$$\left| \frac{\partial \bar{\Phi}_i}{\partial \bar{x}_j} \right| = \left| \overline{\frac{\partial \Phi_i}{\partial x_j}} \right| \cdot |u_{ij}|,$$

und demnach unterscheidet sich die Resultante des Systems

$$\bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}, \; \left| \frac{\partial \bar{\Phi}_i}{\partial \bar{x}_j} \right|$$

nur durch das Hinzutreten einer Potenz von $|u_{ij}|$ von der Resultante des Systems

$$\bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}, \left|\frac{\partial \bar{\Phi}_i}{\partial x_j}\right|;$$

diese entsteht aber durch die Transformation (T) aus der Resultante von

$$\Phi_1, \ldots, \Phi_{m+1}, \left|\frac{\partial \Phi_i}{\partial x_j}\right|;$$

es findet demnach zwischen diesen Resultanten ein ebensolcher Zusammenhang statt. Es ist also:

$$\text{Res.}\left(\bar{\Phi}_1, \ldots, \bar{\Phi}_m, \left|\frac{\partial \bar{\Phi}_i}{\partial \bar{x}_j}\right|\right) = |u_{ij}|^K \text{Res.}\left(\Phi_1, \ldots, \Phi_m, \left|\frac{\partial \Phi_i}{\partial x_j}\right|\right).$$

Wenn man die auf beiden Seiten hier auftretenden Resultanten in der durch den letzten Satz in § 26 gegebenen Gestalt schreibt, entsteht hieraus:

$$\text{Res.}(\bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}) \,\text{Dscr.}(\bar{\Phi}_1, \ldots, \bar{\Phi}_m) = \\ = |u_{ij}|^K \,\text{Res.}(\Phi_1, \ldots, \Phi_{m+1}) \,\text{Dscr.}(\Phi_1, \ldots, \Phi_m).$$

Nun unterscheiden sich

$$\text{Res.}(\bar{\Phi}_1, \ldots, \bar{\Phi}_{m+1}) \text{ und } \text{Res.}(\Phi_1, \ldots, \Phi_{m+1})$$

im Sinne des § 12 nur durch eine als Faktor auftretende Potenz von $|u_{ij}|$. Es besteht demnach auch zwischen den beiden Discriminanten ein ähnlicher Zusammenhang, d. h. ebenso wie die Resultante besitzt auch die Discriminante die durch folgende Identität ausgedrückte Invarianteneigenschaft:

$$\bar{D} = \text{Dscr.}(\bar{\Phi}_1, \ldots, \bar{\Phi}_m) = |u_{ij}|^{N(\Sigma n_i - m)} D.$$

Die hier gegebene genaue Bestimmung des Exponenten für $|u_{ij}|$ erhellt daraus, daß für Formen gegebener Dimension dieser Exponent sich nicht ändert, wenn die $a_y^{(i)}$ wie immer gewählt sind. Nimmt man also Produkte linearer Formen

und benutzt die für diesen Fall gegebene Produktform der Discriminante (§ 23), so sieht man, daß zu jeder als Faktor auftretenden Determinante bei der Transformation genau $|u_{ij}|$ hinzutritt, und erhält demnach in der Anzahl jener Faktoren $N(\Sigma n_i - m)$ den gesuchten Exponenten.

Die Multiplizität der Lösungen.

§ 28. Die für das Formensystem Φ_i dargelegten Eigenschaften der Discriminante sollen nun auf das Gleichungssystem $\Phi_i = 0$ übertragen werden. Es empfiehlt sich, dabei die Fälle eines bestimmten und eines unbestimmten Systems zu sondern.

Wir beschäftigen uns zuerst mit dem strengen und rein algebraischen Beweise des Satzes:

Die Discriminante eines bestimmten Systems $\Phi_i(x_1, \ldots, x_{m+1})$ $(i = 1, \ldots, m)$ wird dann und nur dann Null, wenn das System eine mehrfache Lösung besitzt.

Der Annahme eines bestimmten Systems entsprechend, ist (§ 14) $\overline{R}_{m+1}(u)$ von Null verschieden, und wegen der Invarianteneigenschaft der Resultante genügt es andrerseits, für die Größen u_{ij} irgend ein solches Wertsystem zu setzen, für welches $|u_{ij}| \neq 0$ wird. Wählt man die u_{ij} ferner noch so, daß $\overline{R}_{m+1}(u)$ von Null verschieden wird, so ist alles auf die Betrachtung eines Gleichungssystems

$$F_i(x_1, \ldots, x_m) = 0 \qquad (i = 1, \ldots, m)$$

zurückgeführt, dessen Eliminante in $z = \Sigma t_j x_j$ die Gleichung

$$E(z) = R_{m+1} z^N + R'_{m+1} z^{N-1} + \cdots + R^{(N)}_{m+1} = 0$$

liefert, wo $R^{(k)}_{m+1}$ eine homogene Form k^{ter} Dimension der t ist, mit Koeffizienten, die jenem Rationalitätsbereiche angehören, dem die Formen F_i entstammen; insbesondere ist R_{m+1} eine von Null verschiedene Größe dieses Rationalitätsbereichs.

Nun besitzt das vorgelegte System dann und nur dann eine mehrfache Lösung, wenn die Anzahl der Wurzeln der

Gleichung $E(z) = 0$ kleiner als N wird, also diese Gleichung mehrfache Wurzeln besitzt, oder endlich Dscr. $E(z)$ verschwindet. Dabei ist selbstverständlich Dscr. $E(z)$ als Form der t aufzufassen.

Die somit im Sinne des § 15 bestimmten Wurzelsysteme der Gleichungen $F_i = 0$ seien

$$\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk} \qquad (k = 1, \ldots, \nu),$$

wo $\nu \leqq N$, und die beiden Fälle $\nu < N$, $\nu = N$ zu sondern sind.

Wegen

$$F_i(\xi_{1k}, \xi_{2k}, \ldots, \xi_{mk}) = 0$$

kann man

$$F_i(x_1, \ldots, x_m) = \sum_{j=1}^{m} (x_j - \xi_{jk})\, G_{ij}(x, \xi^{(k)}) \qquad (i = 1, \ldots, m)$$

schreiben, wo in leicht verständlicher Abkürzung

$$G_{ij}(x, \xi^{(k)}) = G_{ij}(x_1, \ldots, x_m, \xi_{1k}, \ldots, \xi_{mk})$$

sein soll.

Die G_{ij} können in mannigfacher Weise gewählt werden, z. B. so, daß in der Entwicklung von F_i nach Potenzprodukten der $x_j - \xi_{jk}$ zuerst alle Glieder, die $x_1 - \xi_{1k}$ enthalten, in der Gestalt $(x_1 - \xi_{1k})\, G_{i1}$ zusammengefaßt werden, von den zurückbleibenden Gliedern wieder alle, die $x_2 - \xi_{2k}$ enthalten, in der Gestalt $(x_2 - \xi_{2k})\, G_{i2}$ geschrieben werden u. s. w. Wie immer aber diese Wahl der G_{ij} erfolge, ist nach Kap. II. § 5 jedenfalls

$$G_{ij}(\xi^{(k)}, \xi^{(k)}) = F_{ij}(\xi^{(k)}), \quad F_{ij} = \frac{\partial F_i}{\partial x_j}.$$

Es sei noch die aus den G_{ij} gebildete Determinante

$$|\, G_{ij}(x, \xi^{(k)})\,|_{(i,j=1,\cdots,m)} = H(x, \xi^{(k)}),$$

dann wird bei entsprechender Bezeichnung der Unterdeterminanten

$$H(x, \xi^{(k)})\,(x_j - \xi_{jk}) = \sum_{i=1}^{m} H_{ij}(x, \xi^{(k)})\, F_i(x_1, \ldots, x_m)$$

und da, wenn $x_j = \xi_{jh}$ gesetzt wird und $h \neq k$ ist, die rechte

Seite verschwindet, während die Größen $\xi_{jh} - \xi_{jk}$ nicht sämtlich Null sind, muß schließlich

$$H(\xi^{(h)}, \xi^{(k)}) = 0 \qquad (h \neq k)$$

sein, während nach dem Vorhergehenden:

$$H(\xi^{(k)}, \xi^{(k)}) = |F_{ij}(\xi^{(k)})| = J(\xi^{(k)}).$$

Schreibt man jedes Wurzelsystem $\xi_{1k}, \ldots, \xi_{mk}$ seiner Multiplizität c_k entsprechend, c_k-mal, so entsteht ein System von mN Größen

$$\xi_{1r}, \xi_{2r}, \ldots, \xi_{mr} \qquad (r = 1, \ldots, N)$$

und eine Determinante

$$\Delta = |H(\xi^{(h)}, \xi^{(k)})|_{(h,k=1,\cdots,N)},$$

die gewiß verschwindet, wenn zwei Wurzelsysteme $\xi^{(h)}$ und $\xi^{(k)}$ nicht verschieden sind, da dann die h^{te} und k^{te} Zeile gleich sind. Für den Fall N verschiedener Wurzelsysteme sind nur die in der Hauptdiagonale stehenden Elemente von 0 verschieden, und der Wert der Determinante:

$$\prod_{k=1}^{N} |F_{ij}(\xi^{(k)})|.$$

Daraus folgt aber, daß in dem jetzt betrachteten Falle, wo es keine mehrfachen Wurzeln gibt und $R_{m+1} \neq 0$ ist, immer

$$\Delta = \prod_{k=1}^{N} F_{ij}(\xi^{(k)})$$

ist. Es ist augenscheinlich Δ eine symmetrische Form der Wurzelsysteme $\xi^{(i)}$, denn wenn $\xi^{(h)}$ und $\xi^{(k)}$ vertauscht werden, so wechseln in Δ die h^{te} und k^{te} Zeile und ebenso die h^{te} und k^{te} Spalte zugleich ihre Plätze; ebensowenig ändert sich das rechts stehende Produkt.

Es ist also in den Bezeichnungen des § 20

$$\Delta = \frac{\varphi(r_0, \ldots, r_{kl}, \ldots)}{r_0^a}$$

$$\prod_{k=1}^{N} F_{ij}(\xi^{(k)}) = \frac{\psi(r_0, \ldots, r_{kl}, \ldots)}{r_0^b}$$

wo φ und ψ homogene Formen bedeuten und $r_0 = R_{m+1}$ ist, und nun besteht gewiß die Gleichung

$$r_0^b \varphi = r_0^a \psi,$$

wenn Dscr. $E(z)$ nicht Null ist.

Führt man diese Betrachtung für das allgemeine Gleichungssystem durch, so besteht demnach diese Gleichung für jedes Koeffizientensystem $a_g^{(i)}$, für welches nicht r_0 und die sämtlichen Koeffizienten der Form Dscr. $E(z)$ zugleich Null sind, also gewiß für jedes Koeffizientensystem, für welches $r_0 A$, wo A irgend einen Koeffizienten der Form Dscr. $E(z)$ bezeichnet, von 0 verschieden ist. Dann gilt sie aber für jedes Koeffizientensystem, und da r_0 als von Null verschieden vorausgesetzt ist, hat man endlich die allgemein gültige Bestimmung

$$r_0^{\Sigma n_i - m - 1} \Delta = r_0^{\Sigma n_i - m - 1} \prod_{k=1}^{N} F_{ij}(\xi^{(k)}) = \text{Dscr.}(F_1, \ldots, F_m).$$

Die Discriminante verschwindet also unbedingt, wenn $R_{m+1} \neq 0$ und zwei Wurzelsysteme $\xi^{(h)}$ und $\xi^{(k)}$ nicht verschieden sind, oder also eine mehrfache Lösung vorhanden ist, wie dies die vorstehende Gleichung evident zeigt, da ja in diesem Falle Δ gleich Null ist.

§ 29. Um den in § 28 angezeigten Satz vollständig zu beweisen, ist nun noch umgekehrt zu zeigen, daß aus dem Verschwinden der Discriminante immer auch die Existenz einer mehrfachen Lösung folgt (wo wir wieder $R_{m+1} = r_0 \neq 0$ voraussetzen).

Man erschließt diese Tatsache aus dem Umstande, daß die Eliminante $E(z)$ nach § 15 die Resultante des Systems

$$F_1, \ldots, F_m, z - \sum t_j x_j$$

ist, also die Kongruenz

$$E(z) \equiv 0 \ (\text{mod. } F_1, \ldots, F_m, z - \sum t_j x_j)$$

besteht, aus der die Identität

$$E\left(\sum_{j=1}^{m} t_j x_j\right) = \sum_{i=1}^{m} K_i F_i$$

folgt. Behält man z als Abkürzung für $\sum_{j=1}^{m} t_j x_j$, so ergibt sich, indem man nach x_j deriviert:

$$\frac{\partial E}{\partial z} t_j = \sum_{i=1}^{m} \frac{\partial K_i}{\partial x_j} F_i + \sum_{i=1}^{m} K_i F_{ij}.$$

Ist nun $\xi^{(k)}$ ein Wurzelsystem, für welches $|F_{ij}(\xi^{(k)})| = 0$ wird, so seien die Unterdeterminanten niedrigsten Grades, die noch sämtlich verschwinden, die vom r^{ten} Grade.

Wenn $r = 1$, also $F_{ij}(\xi^{(k)})$ immer gleich Null ist, so folgt aus der letzten Identität, daß auch $\frac{\partial E}{\partial z} = 0$ die Wurzel $z = \sum t_j \xi_{jk}$ besitzt, und diese Wurzel also, wie behauptet, eine mehrfache Wurzel von $E(z) = 0$ ist.

Ist $r > 1$, so erhält man durch passende Wahl der Unterdeterminanten $r - 1^{\text{ten}}$ Grades, indem man mit diesen, darunter einer nicht verschwindenden, multipliziert

$$\frac{\partial E}{\partial z} \sum t_j d_j = \sum_{i=1}^{m} K_i F_i;$$

und wenn man wieder $x_j = \xi_{jk} (j = 1, \ldots, m)$ setzt, da ein d_j gewiß von Null verschieden ist, $\frac{\partial E}{\partial z} = 0$ für $z = \Sigma t_j \xi_{jk}$; also ergibt sich wieder $z = \Sigma t_j \xi_{jk}$ als mehrfache Wurzel von $E(z) = 0$.

Damit ist aber der Satz des § 28 vollständig bewiesen.

§ 30. Die bisher durchgeführten Entwicklungen gelangen endlich zum Abschluß durch den Nachweis, daß die Discriminante eines unbestimmten Systems immer verschwindet.

Ein unbestimmtes System ist ein solches, das unendlich viele wirkliche Lösungen besitzt. Es muß demnach unendlich viele Lösungen geben, in denen eine und dieselbe Unbestimmte von Null verschiedene Werte hat. Gäbe es immer nur eine

endliche Anzahl von Lösungen, in denen der Reihe nach $x_1, \ldots, x_{m+1}$ von Null verschieden ist, so wäre eben die Gesamt-Anzahl der Lösungen auch endlich. Wenn wir diese Unbestimmte mit x_{m+1} bezeichnen, so involviert dies nur eine Änderung in der Benennung der Unbestimmten, und es kann also schließlich angenommen werden, daß das Gleichungssystem

$$F_i(x_1, \ldots, x_m) = 0$$

unendlich viele (endliche) Wurzelsysteme besitzt; d. h. dem Systeme $F_i = 0$ genügt eine Mannigfaltigkeit, deren Stufenzahl kleiner als m ist.

Wir können weiter annehmen, daß das System $F_i = 0$ durch eine an den $x_1, \ldots, x_m$ ausgeführte homogene lineare Transformation mit nicht verschwindender Determinante im Sinne des Kap. V. von Zufälligkeiten befreit ist; denn die Discriminanten des ursprünglichen und des transformierten Systems sind zugleich Null, oder von Null verschieden.

Bei Benutzung der in Kap. V. § 9 benutzten Bezeichnungen*) ersieht man, daß dem Gleichungssystem $\Delta_a F_i = 0$ genügt wird, wenn man $x_{h+1}, \ldots, x_{m-1}$ als Unbestimmte beläßt, x als algebraische Funktion dieser Unbestimmten aus

$$\varphi(x, a_1, \ldots, a_m, x_{h+1}, \ldots, x_{m-1}) = 0 \qquad (1)$$

bestimmt und dann $x_1, \ldots, x_h$ aus

$$\left[\frac{\partial \varphi}{\partial x}\right]_a x_i + [\varphi_i]_a = 0 \qquad (i = 1, \ldots, h) \qquad (2)$$

bestimmt, während sich x_m aus

$$x = \sum_{i=1}^{m} a_i x_i \text{ oder } \left[\frac{\partial \varphi}{\partial x}\right]_a x_m + [\varphi_m]_a = 0 \qquad (3)$$

---

*) Daß hier die Ausführungen der allgemeinen Eliminationstheorie eintreten, ist naturgemäß und nicht vielleicht die Folge der „künstlichen" Vermeidung von Stetigkeitsbetrachtungen. Die „Stetigkeit" der in einer Mannigfaltigkeit von niedrigerer als m^{ter} Stufe vereinigten Wurzelsysteme kann ja eben nur aus jener Darstellung der Mannigfaltigkeit gefolgert werden.

bestimmt. (Dabei ist $h < m - 1$, also die so definierte Mannigfaltigkeit $V^{(h+1)}$ von höchstens $m - 1^{\text{ter}}$ Stufe).

Es ist ferner $\varphi(x, t_1, \ldots, t_m, x_{h+1}, \ldots, x_{m-1})$ als irreduzibel vorauszusetzen, und die für t_i einzusetzenden Werte a_i sind so gewählt, daß die Discriminante Δ_a von

$$\varphi(x, a_1, \ldots, a_m, x_{h+1}, \ldots, x_{m-1})$$

eine von 0 verschiedene Form von $x_{h+1}, \ldots, x_{m-1}$ ist.

Dann hat man für Δ_a auch die Relation

$$\Delta_a = \lambda\varphi + \mu\left[\frac{\partial\varphi}{\partial x}\right]_a;$$

also

$$\Delta_a x_i + \mu[\varphi_i]_a = 0, \qquad (i = 1, \ldots, h)$$

sowie $\Delta_a F_i = 0$, wenn jene Werte von $x_1, \ldots, x_h, x_m$ eingesetzt werden, und x die in (1) definierte algebraische Funktion bedeutet, während

$$\sum_{i=1}^{m} a_i x_i = x$$

zu setzen ist. Das letztere bedeutet aber wieder nur eine homogene lineare Transformation der Unbestimmten in F_i; geht durch diese F_i in $G_i(x, x_1, \ldots, x_{m-1})$ über, so ist Dscr. $(G_1, \ldots, G_m)$ und Dscr. $(F_1, \ldots, F_m)$ wieder zugleich Null oder von Null verschieden.

Multipliziert man mit einer genügend hohen Potenz von Δ_a, sodaß $\Delta_a^{c_i} G_i$ die Größen $x_1, \ldots, x_h$ nur mehr in den Produkten $\Delta_a x_1, \ldots, \Delta_a x_h$ enthält, so wird

$$\Delta_a^{c_i} G_i \equiv H_i(x, x_{h+1}, \ldots, x_{m-1}) (\text{mod.} \ldots, \Delta_a x_i + \mu[\varphi_i]_a, \ldots)$$

und H_i gleich Null, wenn x jene durch (1) definierte algebraische Funktion ist, also auch H_i durch φ teilbar. Hieraus folgt endlich die Kongruenz

$$\Delta_a^{c_i} G_i \equiv 0 \,(\text{mod. } \psi_1, \ldots, \psi_h, \psi_{h+1}), \qquad (C)$$

wenn zur Abkürzung

$$\psi_i = \Delta_a x_i + \mu[\varphi_i]_a, \qquad (i = 1, \ldots, h)$$
$$\psi_{h+1} = \varphi$$

gesetzt wird; und die Anzahl der Elemente des in (C) auftretenden Modulsystems ist $h+1<m$. Wir schreiben (C) noch in der Gestalt

$$\Delta_a^{c_i} G_i = \sum_{j=1}^{m} C_{ij}\psi_j,$$

wo $\psi_{h+2}, \ldots, \psi_m$ einfach gleich Null anzunehmen sind, und erhalten hieraus

$$\Delta_a^{c_i}\frac{\partial G_i}{\partial x_r} = \sum_{j=1}^{m}\frac{\partial C_{ij}}{\partial x_r}\psi_j + \sum_{j=1}^{m} C_{ij}\frac{\partial \psi_j}{\partial x_r} + G_i\frac{\partial \Delta_a^{c_i}}{\partial x_i} \quad (r=0,1,\ldots m-1),$$

also für die Elemente der in (1), (2) definierten Mannigfaltigkeit, wo $\psi_j = 0$ ist,

$$\Delta_a^{c_i}\frac{\partial G_i}{\partial x_r} = \sum_{j=1}^{m} C_{ij}\frac{\partial \psi_j}{\partial x_r}$$

und endlich für dieselben Elemente

$$\Delta_a^{c_1+\cdots+c_m}\left|\frac{\partial G_i}{\partial x_r}\right| = |C_{ij}|\left|\frac{\partial \psi_j}{\partial x_r}\right|;$$

da aber rechts wenigstens ein ψ_j identisch Null ist, und daher für $\left|\frac{\partial \psi_j}{\partial x_r}\right|$ dasselbe stattfindet, ferner Δ_a eine von Null verschiedene Form der Unbestimmten ist, hat man endlich für alle Elemente jener Mannigfaltigkeit $\left|\frac{\partial G_i}{\partial x_r}\right| = 0$.

Nun ist aber

$$\text{Dscr.}\,(G_1, \ldots, G_m) \equiv 0 \left(\text{mod. } G_1, \ldots, G_m, \left|\frac{\partial G_i}{\partial x_r}\right|\right),$$

und wenn man irgend ein Element jener Mannigfaltigkeit rechts für $x, x_1, \ldots, x_{m-1}$ einsetzt, $x_{h+1}, \ldots, x_{m-1}$ immer als Unbestimmte aufgefaßt, so wird jedes Element des Modulsystems, also auch die Discriminante der G und damit endlich noch die Discriminante des Systems $F_1, \ldots, F_m$ gleich Null, was zu beweisen war.

Wir können nun leicht die Entwicklung der §§ 28 und 30 in Folgendem zusammenfassen:

Das System $\Phi_i = 0$, $(i = 1, \ldots, m)$ hat „im allgemeinen“ N verschiedene Lösungen; dem gegenüber nennen wir das System singulär, wenn die Anzahl der verschiedenen Lösungen entweder kleiner als N ist, also „mehrfache“ Lösungen existieren, oder aber die Anzahl der verschiedenen Lösungen größer als N, also unendlich groß wird. Dann haben wir den Satz:

Das Verschwinden der Discriminante der Formen $\Phi_i (i = 1, \ldots, m)$ ist die notwendige und hinreichende Bedingung dafür, daß das Gleichungssystem $\Phi_i = 0$ ein singuläres sei.

Der durchweg ausgeschlossene Fall eines Systems linearer Formen läßt sich, wie unmittelbar klar, elementar erledigen. Ein solches Gleichungssystem, dessen Koeffizienten eine Matrix von m Zeilen und $m + 1$ Spalten ergeben, ist dann und nur dann singulär, wenn jede daraus sich ergebende Determinante m^{ten} Grades verschwindet.

Siebentes Kapitel.

Lineare diophantische Probleme.

(Allgemeine Sätze und die algebraische Theorie.)

Aufstellung des Problems.

§ 1. Es sei A irgend ein holoider Bereich, der ebensowohl ein echter holoider Bereich, wie auch ein orthoider Bereich sein kann, und $[\mathsf{A}, x_1, \ldots, x_m]$ ein diesem entstammender Formenbereich. Sind

$$F_{i0}, F_{i1}, \ldots, F_{il} \qquad (i = 1, \ldots, k)$$

diesem Bereiche angehörige gegebene Formen, so sollen demselben Bereiche angehörige Formen

$$X_1, \ldots, X_l$$

bestimmt werden, die dem Gleichungssysteme

$$F_{i0} = F_{i1} X_1 + F_{i2} X_2 + \cdots + F_{il} X_l, \qquad (I)$$
$$(i = 1, \ldots, k)$$

genügen. In dieser Auffassung ist (I) ein System linearer diophantischer Gleichungen, wo also im Gegensatze zur bisherigen Fragestellung nur jene Größen als Lösungen in Betracht kommen, die dem Formenbereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehören.

Es werden im Folgenden insbesondere zwei Fälle in Betracht zu ziehen sein, erstens, wenn A ein orthoider Bereich, zweitens, wenn A der Bereich der rationalen und ganzen Zahlen ist. Im ersten Falle gehört das Problem der Algebra, im

zweiten Falle der Arithmetik an, wenn wir diese Disziplinen im Sinne der Auseinandersetzungen des Kap. IV. § 8 sondern. Auf diese beiden fundamentalen Fälle gehen alle hierher gehörigen Probleme zurück, die in der Theorie der algebraischen Größen auftreten.

Das Problem der Auflösung eines linearen diophantischen Gleichungssystems reduziert sich in diesen Fällen auf zwei einfachere Fundamentalprobleme, und diese Reduktion soll — um Wiederholungen zu vermeiden — hier sogleich in etwas allgemeinerer Form dargelegt werden.

Ist Γ irgend ein holoider Bereich, so verstehn wir unter der „Auflösung des Systems linearer diophantischer Gleichungen

$$\sum_{j=1}^{l} \gamma_{ij} \xi_j = \gamma_{i0} \qquad (i = 1, \ldots, k), \quad \text{(II)}$$

in Γ", wo die γ dem Bereiche Γ angehören, die Bestimmung aller demselben Bereiche angehörigen Größensysteme $\xi_1, \ldots, \xi_l$, die dem Gleichungssysteme genügen. An Stelle der „Bestimmung" tritt, wenn unendlich viele solche Systeme existieren, die Forderung, dieselben in bestimmter Weise vollständig zu beschreiben.

Der Bereich Γ soll kurzweg als diophantischer Bereich bezeichnet werden, wenn für jede homogene lineare diophantische Gleichung

$$\gamma_1 \xi_1 + \gamma_2 \xi_2 + \cdots + \gamma_l \xi_l = 0 \qquad (1)$$

eine endliche Anzahl von dem Bereiche angehörigen Größensystemen

$$\xi_{1h}, \xi_{2h}, \ldots, \xi_{lh}, \qquad (h = 1, \ldots, r) \quad (2)$$

bestimmt werden kann, so daß nicht nur:

$$\xi_j = \mu_1 \xi_{j1} + \mu_2 \xi_{j2} + \cdots + \mu_r \xi_{jr}, \qquad (j = 1, \ldots, l), \quad (3)$$

wenn für $\mu_1, \ldots, \mu_r$ beliebige Größen aus Γ gesetzt werden, eine Lösung jener diophantischen Gleichung gibt, sondern umgekehrt auch jede Lösung $\xi_1, \ldots, \xi_l$ auf diese Gestalt gebracht

werden kann. Diese Eigenschaft drücken wir in folgenden Worten aus: In einem diophantischen Bereiche bilden die Lösungen jeder homogenen diophantischen Gleichung eine endliche Schar. Die Schar heißt im Anschluß an frühere Bezeichnungen (Kap. V. § 13) eine r-gliedrige. Mit den Größensystemen (2) sind selbstverständlich die Systeme (3) bei beliebiger Wahl der μ_i auch Lösungen, aber es ist, wenn für Γ keine weitere Festsetzung vorliegt, die Möglichkeit durchaus nicht ausgeschlossen, daß jene r Systeme, wie groß man auch r wähle, niemals genügen, um in (3) sämtliche Lösungen zu geben. Für einen „diophantischen" Bereich tritt eben dieser Fall nicht auf. In diesem Sinne wird später noch zu zeigen sein, daß jeder Formenbereich, der einem orthoiden Bereiche oder dem Bereiche [1] entstammt, ein diophantischer Bereich ist.

Für einen diophantischen Bereich reduziert sich die vollständige Auflösung eines Systems linearer diophantischer Gleichungen (II) auf die zwei folgenden Fundamentalprobleme:

1) Bestimmung der endlichen Schar, die einer einzelnen homogenen linearen diophantischen Gleichung (1) genügt.

2) Entscheidung der Lösbarkeit für eine lineare diophantische Gleichung von der Gestalt:

$$\gamma_1 \xi_1 + \cdots + \gamma_l \xi_l = 1 \qquad (4)$$

und Bestimmung einer Lösung, wenn eine solche vorhanden ist.

Wie nach Erledigung dieser beiden Aufgaben die vollständige Lösung eines jeden linearen diophantischen Systems in einer endlichen Anzahl von Schritten erfolgt, soll nun dargelegt werden.

Vor allem ist es klar, daß nach Kenntnis einer Lösung von (4) die Gesamtheit dieser Lösungen vollständig beschrieben werden kann. Ist diese Lösung

$$\xi_{10}, \cdots, \xi_{l0},$$

so genügt jede andere Lösung der homogenen Gleichung

$$\gamma_1(\xi_1 - \xi_{10}) + \gamma_l(\xi_l - \xi_{l0}) = 0,$$

und es ist demnach die Gesamtheit der Lösungen in der Gestalt

$$\xi_j = \xi_{j0} + \mu_1\xi_{j1} + \cdots + \mu_r\xi_{jr} \qquad (j = 1, \ldots, l) \quad (5)$$

darstellbar, wo die μ beliebige Größen aus Γ sind.

Ist zweitens die Gleichung

$$\gamma_1\xi_1 + \cdots + \gamma_l\xi_l = \gamma$$

vorgelegt und γ von 1 verschieden, so sind die Lösungen dieser Gleichung unter denen der Gleichung

$$\gamma_1\xi_1 + \cdots + \gamma_l\xi_l - \gamma\eta = 0$$

enthalten, und zwar in der Weise, daß jede Lösung der letzten Gleichung, in der $\eta = 1$ ist, eine Lösung der vorgelegten Gleichung ergibt und umgekehrt. Nun hat aber in der allgemeinen Lösung der letzteren Gleichung η die Gestalt

$$\eta = \mu_1\eta_1 + \cdots + \mu_r\eta_r,$$

und es sind also nur noch die Größen μ der Bedingung

$$\mu_1\eta_1 + \cdots + \mu_r\eta_r = 1$$

gemäß zu bestimmen. Dies gibt für die μ ähnlich wie (4) gebaute Ausdrücke, und als allgemeine Lösung der Gleichung

$$\xi_j = \xi'_{j0} + \nu_1\xi'_{j1} + \cdots + \nu_s\xi'_{js} \qquad (j = 1, \cdots, l), \quad (6)$$

wo die ν wieder beliebige Größen aus Γ sind.

Daß nun auch die allgemeine Lösung des diophantischen Systems (II) in einer endlichen Anzahl von Schritten aufgestellt werden kann, erschließt man in einfacher Weise durch den Übergang von k zu $k - 1$. Hat man nämlich für die erste der Gleichungen in (II):

$$\sum_{j=1}^{l}\gamma_{1j}\xi_j = \gamma_{10}$$

die allgemeine Lösung in der Gestalt von (6) gefunden, so ergeben sich, wenn man diese Darstellung der ξ_j in die übrigen

Gleichungen einsetzt, notwendige und hinreichende Bedingungsgleichungen für die Größen v, die geradezu ein System von $k-1$ linearen diophantischen Gleichungen für diese Größen geben. In dieser Weise fortfahrend, gelangt man schließlich zu einer Gleichung und zu einer definitiven Darstellung der Gesamtheit der Lösungen von (II), die wieder die in (6) charakterisierte Gestalt hat.

Modul- oder Divisorensysteme.

§ 2. Bevor wir die Lösung des aufgestellten Problems weiter verfolgen, muß noch eine weitere sich daran knüpfende Begriffsbildung vorgetragen werden, die für die Theorie der algebraischen Größen von fundamentaler Bedeutung ist und deshalb am besten von vornherein in der Fassung der hierher gehörigen Resultate verwendet wird.

Die Tatsache, daß die lineare diophantische Gleichung

$$F = F_1 X_1 + \cdots + F_l X_l$$

in dem Formenbereiche $[\mathsf{A}, x_1, \ldots, x_m]$ eine Lösung besitzt, wird, wenn man von der Bestimmung der Größen $X_1, \ldots, X_l$ absieht, auch durch die Kongruenz

$$F \equiv 0 \pmod{F_1, \ldots, F_l}$$

ausgedrückt, wo selbstverständlich wieder der Formenbereich, in dem diese Tatsache statuiert wird, ein für allemal festgesetzt ist*).

Für $l = 1$ sagt diese Behauptung nichts anderes, als daß F im Formenbereiche $[\mathsf{A}, x_1, \ldots, x_m]$ durch F_1 teilbar ist; wir haben es demnach im allgemeinen Falle mit einer Erweiterung des Teilbarkeitsbegriffs zu tun, wo an Stelle

*) Daß die Richtigkeit dieser Aussage von der Wahl des Bereichs abhängig ist, zeigt ein einfaches Beispiel. Es ist z. B.

$$1 \equiv 0, \pmod{x+2, x+4}$$

im Bereiche der rationalen Formen; dieselbe Behauptung ist aber falsch im Bereiche der rationalen und ganzen Formen.

des Teilers oder eingliedrigen Moduls F_1 das l-gliedrige Modulsystem $(F_1, \ldots, F_l)$ tritt, das in dieser Auffassung nun auch — nach Kronecker — als Divisorensystem*) bezeichnet wird.

In Verfolgung dieser Analogie drücken wir endlich die durch die Kongruenz

$$F \equiv 0 \pmod{F_1, \cdots, F_l}$$

gegebene Eigenschaft von F auch so aus, daß F das Modulsystem (oder Divisorensystem) $(F_1, \ldots, F_l)$ enthält**).

Die naturgemäße Erweiterung dieser Ausdrucksweise führt zu folgenden Definitionen:

I. Das Modulsystem (Divisorensystem) $(M_1, \ldots, M_h)$ enthält das Modulsystem $(N_1, \ldots, N_g)$, wenn dies für jedes Element des ersten Modulsystems der Fall ist, also, wenn in der Kongruenzbezeichnung

$$M_i \equiv 0 \pmod{N_1, \ldots, N_g} \qquad (i = 1, \ldots, h).$$

II. Zwei Modulsysteme (Divisorensysteme) heißen äquivalent, wenn jedes von ihnen das andere enthält. In Zeichen soll dies durch

$$(M_1, \ldots, M_h) \simeq (N_1, \ldots, N_g)$$

ausgedrückt werden; für den Fall $h = 1$, $g = 1$ hat das Zeichen $\simeq$ dann genau die Bedeutung des früher gebrauchten Zeichens $\sim$.

Man erhält hieraus unmittelbar den einfachen Satz: Wenn M das Modulsystem $(M_1, \ldots, M_h)$ enthält, so ist $(M_1, \ldots, M_h) \simeq (M, M_1, \ldots, M_h)$.

Ein echtes Modulsystem ist ein solches, das in der absoluten Einheit nicht enthalten ist, für welches also die Aqui-

*) Kronecker, Festschrift, § 20.

**) Das in Kap. I behandelte Beispiel des Bereichs $[\sqrt{-5}]$, insbesondere § 9 zeigt, daß diese Begriffsbildung auch schon dann für den Ausdruck gewisser Tatsachen notwendig sein kann, wenn man im Bereiche [A] verbleibt, ohne weitere Unbestimmte hinzuzufügen, wenn also $F, F_1, \ldots, F_l$ durchweg Größen des Bereichs [A] sind.

valenz $(M_1, \ldots, M_h) \simeq 1$ nicht besteht. Jedes in der absoluten Einheit nicht enthaltene oder echte Modulsystem bestimmt demnach (Kap. I. § 10) einen echten Kongruenzbereich.

Auch der Begriff des größten gemeinschaftlichen Teilers läßt sich unmittelbar auf die Modul- oder Divisorensysteme übertragen. (Wir benutzen nun, wo die Beziehung zum Kongruenzbereich zurücktritt und wir es mit den Eigenschaften dieser Größensysteme an sich zu tun haben, vorzugsweise die letztere Benennung.) Dies geschieht durch folgende Festsetzung:

III. Das Divisorensystem $(M_1, \ldots, M_h, N_1, \ldots, N_g)$ heißt der größte gemeinschaftliche Inhalt der Divisorensysteme $(M_1, \ldots, M_h)$ und $(N_1, \ldots, N_g)$ und wird durch die Eigenschaft charakterisiert, daß jedes Divisorensystem, das in dem ersten enthalten ist, auch in dem zweiten und dritten Divisorensystem enthalten ist und auch umgekehrt. Diese Behauptung ist aus den betreffenden Definitionen unmittelbar klar. Jedes Divisorensystem, das die soeben ausgesprochene Eigenschaft besitzt, muß $\simeq (M_1, \ldots, M_h, N_1, \ldots, N_k)$ sein, denn es enthält dieses Divisorensystem und ist auch in diesem enthalten. Der größte gemeinsame Inhalt zweier Divisorensysteme ist also im Sinne der jetzt gegebenen Äquivalenzbestimmung eindeutig gegeben.

IV. Die beiden Divisorensysteme $(M_1, \ldots, M_h)$ und $(N_1, \ldots, N_g)$ sollen relativ prim heißen, wenn ihr größter gemeinschaftlicher Inhalt $(M_1, \ldots, M_h, N_1, \ldots, N_g) \simeq 1$ ist.

Für die schärfere Sonderung der Begriffe — insbesondere in unsern Formeln — ist die Einführung des Zeichens $\simeq$ von Vorteil. Es bedeutet eine engere Äquivalenz als das früher gebrauchte Zeichen $\sim$. In folgerichtigem Anschluß an die bisherige Anwendung dieses Zeichens soll

$$(M_1, \ldots, M_h) \sim (N_1, \ldots, N_g)$$

besagen, daß jeder gemeinschaftliche Teiler von $M_1, \ldots, M_h$ auch ein gemeinschaftlicher Teiler von $N_1, \ldots, N_g$ ist und

umgekehrt, und dies kann ganz gut der Fall sein, ohne daß zugleich

$$(M_1, \ldots, M_h) \simeq (N_1, \ldots, N_g)$$

ist. So hat man z. B. im Bereiche der rationalen und ganzen Formen

$$(x+2, x+4) \sim 1,$$

ohne daß

$$(x+2, x+4) \simeq 1$$

ist, da es keine Formen A und B gibt, für die

$$A(x+2) + B(x+4) = 1$$

wird. Dies hat seinen einfachen Grund darin, daß $x+2$ und $x+4$ das zweigliedrige Divisorensystem $(x, 2)$ enthalten, was für 1 nicht der Fall ist.

Das Zeichen $\simeq$ besagt, wie man unmittelbar sieht, daß jedes in $M_1, \ldots, M_h$ enthaltene Divisorensystem auch in $N_1, \ldots, N_g$ enthalten ist und umgekehrt; bei Anwendung des Zeichens $\sim$ gilt dies nur für gewöhnliche Teiler (eingliedrige Divisorensysteme).

Würde man die Anwendung des Zeichens $\sim$ auf einzelne Größen beschränken, so fiele dieser Unterschied weg, denn aus $M \sim N$ folgt immer auch $M \simeq N$.

Es ist aber nicht ohne Wichtigkeit, diese engere und weitere Äquivalenz in unseren Zeichen auch fernerhin unterscheiden zu können; wir würden auch sonst mit der früher gebrauchten einfachen Bezeichnung des größten gemeinschaftlichen Teilers in Widerspruch geraten.

Wo im folgenden einfach von äquivalenten Divisorensystemen die Rede ist, soll immer die durch das Zeichen $\simeq$ bestimmte engere Äquivalenz verstanden sein.

§ 3. Die Gesamtheit der Divisorensysteme, die wir aus den Größen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ bilden können, werden abermals in einem „Bereiche", dem Divisorenbereiche von $[\mathsf{A}, x_1, \ldots, x_m]$, zusammengefaßt, wenn wir für diese Divisorensysteme eine gewisse gesetzmäßige Verknüpfung festsetzen.

Das Gesetz dieser Verknüpfung, der s. g. Komposition, lautet einfach dahin, daß aus den Divisorensystemen

$(\ldots, M_i, \ldots), (i = 1, \ldots, h)$ und $(\ldots, N_j, \ldots), (j = 1, \ldots, g)$

ein drittes durch

$$(\ldots, M_i N_j, \ldots) \qquad (i = 1, \ldots, h; j = 1, \ldots, g)$$

gegebenes Divisorensystem zu bilden ist.

Wir nennen letzteres System aus den beiden ersten zusammengesetzt oder komponiert; jene Systeme heißen dabei die Kompositionsfaktoren oder (wegen der augenfälligen Analogie mit der Multiplikation eingliedriger Systeme) auch kurz die Faktoren des letzten Systems, das demgemäß auch als Produkt der beiden ersten Systeme bezeichnet wird.

Die Definition der Komposition kann nun auch als Äquivalenz:

$$(\ldots, M_i, \ldots)(\ldots, N_j, \ldots) \simeq (\ldots, M_i N_j, \ldots)$$
$$(i = 1, \ldots, h; j = 1, \ldots, g)$$

geschrieben werden, wenn wir die zu komponierenden Systeme einfach nebeneinander schreiben.

Die Berechtigung dieser Schreibweise folgt aus der Tatsache, daß bei der Komposition äquivalente Systeme einander vollständig vertreten können. Es drückt sich dies in dem unmittelbar ersichtlichen Satze aus, daß aus

$$(M_1, \ldots, M_h) \simeq (M_1', \ldots, M_{h'}')$$

immer auch

$$(\ldots, M_i N_j, \ldots) \simeq (\ldots, M_{i'}' N_j, \ldots)$$
$$(i = 1, \ldots h; i' = 1, \ldots, h'; j = 1, \ldots g)$$

folgt.

Nach ihrer Definition ist für die Komposition das kommutative Prinzip richtig, ebenso wie für die Multiplikation, in die diese neue Verknüpfung für $h = 1$ und $g = 1$ übergeht.

Diese Bestimmungen führen zu dem trotz seiner Einfachheit sehr wichtigen Satze:

Wenn ein Divisorensystem die beiden Systeme $(M_1, \ldots, M_h)$ und $(N_1, \ldots N_g)$ enthält, und diese beiden

relativ prim sind, so enthält es auch das Produkt der beiden Systeme.

Offenbar braucht man den Satz nur für eine einzelne Größe F zu beweisen. Daß jene Systeme relativ prim sind, d. h. daß

$$(M_1, \ldots, M_h, N_1, \ldots, N_g) \simeq 1$$

ist, bedeutet, ausführlich geschrieben, daß es Größen U_i, V_j des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ gibt, für welche

$$\sum_{i=1}^{h} M_i U_i + \sum_{j=1}^{g} N_j V_j = 1$$

wird. Andrerseits ist auch, wenn G_i, H_j abermals Größen des Bereichs $[\mathsf{A}_1 x_1, \ldots, x_m]$ sind:

$$F = \sum_{i=1}^{h} G_i M_i = \sum_{j=1}^{g} H_j N_j$$

und daher:

$$N_j F = \sum_{i=1}^{h} G_i M_i N_j, \qquad (j = 1, \ldots, g)$$

$$M_i F = \sum_{j=1}^{g} H_j M_i N_j, \qquad (i = 1, \ldots, h)$$

also auch, wenn man der Reihe nach mit V_j, U_i multipliziert und addiert:

$$F \equiv 0 \ (\text{mod.} \ldots, M_i N_j, \ldots).$$

Insbesondere folgt noch hieraus der folgende spezielle Satz:

Ist $(M_1, N_1) \simeq 1$, so hat man auch

$$(M_1 N_1, M_2, \ldots, M_h) \simeq (M_1, M_2, \ldots, M_h)(N_1, M_2, \ldots, M_h).$$

Daß das links stehende Divisorensystem das Produkt auf der rechten Seite enthält, ist eine Folge des eben bewiesenen Satzes, denn es enthält augenscheinlich die beiden Faktoren, und diese sind mit M_1 und N_1 auch relativ prim. Daß aber umgekehrt das Produkt rechts jenes Divisorensystem enthält, ist ebenso einfach einzusehn. Die Elemente des als Produkt gegebenen Divisorensystems sind $M_1 N_1$ und weiter nur durch M_2, M_3, ... oder M_h teilbare Größen.

In weiterer Verfolgung der Analogie mit den gewöhnlichen Teilbarkeitssätzen gelangt man noch zu folgendem Satze:

Ist in dem Divisorensysteme $(N_1, \ldots, N_g)$ nicht jedes Element 0, und

$$(\ldots, M_j, \ldots)(\ldots, N_j, \ldots) \simeq (\ldots, M'_{i'}, \ldots)(\ldots, N_j, \ldots),$$
$$(i = 1, \ldots, h;\ i' = 1, \ldots, h';\ j = 1, \ldots, g),$$

so enthält das Divisorensystem $(\ldots, M_i^g, \ldots)$ das System $(\ldots, M'_{i'}, \ldots)$ und $(\ldots, M_i'^g, \ldots)$ auch $(\ldots, M_i, \ldots)$.

Der Annahme nach ist

$$M_i N_s = \sum_{j=1}^{g} L_{ij}^{(s)} N_j, \qquad (s = 1, \ldots, g)$$

wo die $L_{ij}^{(s)}$ lineare Formen der M' sind; also wird auch

$$\sum_{j=1}^{g} (L_{ij}^{(s)} - \delta_{sj} M_i) N_j = 0,$$

wo, wie schon häufig, $\delta_{sj} = 1$, wenn $s = j$, und $\delta_{sj} = 0$, wenn $s \neq j$ ist. Da nun die N_j nicht sämtlich 0 sind, hat man

$$\left| L_{ij}^{(s)} - \delta_{ij} M_i \right|_{(j,s=1,\ldots,g)} = 0,$$

also in der Tat

$$M_i^g \equiv 0 \ (\text{mod.} \ldots, M'_{i'}, \ldots),$$

und genau ebenso

$$M_{i'}'^g \equiv 0 \ (\text{mod.} \ldots, M_i, \ldots,).$$

Insbesondere muß noch der folgende spezielle Fall hervorgehoben werden:

Ist in dem Divisorensysteme $(N_1, \ldots, N_g)$ nicht jedes Element 0, und

$$(\ldots, M_i, \ldots)(\ldots, N_j, \ldots) \simeq (\ldots, N_j, \ldots),$$

so ist auch

$$(\ldots, M_i, \ldots) \simeq 1.$$

Nach dem soeben bewiesenen allgemeinen Satze enthält 1 das Divisorensystem $(\ldots, M_i, \ldots)$, und dieses selbstverständlich auch das „Divisorensystem" 1; es ist also in der Tat

$$(\ldots, M_i, \ldots) \simeq 1.$$

Daß aus den im allgemeinen Satze festgesetzten Bedingungen

$$(\ldots, M_i, \ldots) \simeq (\ldots, M_{i'}, \ldots)$$

durchaus nicht folgt, ist eine merkwürdige Tatsache, die es wohl verdient, durch ein einfaches Beispiel illustriert zu werden.

In dem Formenbereiche $[\mathsf{A}, x, y]$, der einem beliebigen holoiden Bereiche A entstammt, ist

$$(x^2, y^2)(x, y) \simeq (x^3, x^2y, xy^2, y^3),$$
$$(x^2, xy, y^2)(x, y) \simeq (x^3, x^2y, xy^2, y^3);$$

trotzdem sind die Divisorensysteme

$$(x^2, y^2) \text{ und } (x^2, xy, y^2)$$

nicht äquivalent, denn die Kongruenz

$$xy \equiv 0 \pmod{x^2, y^2}$$

ist augenscheinlich unmöglich. Wohl ist aber (x^2, xy, y^2) in (x^4, y^4), und (x^2, y^2) in (x^4, x^2y^2, y^4) enthalten.

§ 4. Daß die Analogie für die Theorie der Divisorensysteme mit derjenigen der gewöhnlichen Teiler (eingliedriger Divisorensysteme) in dieser Weise abbricht, beruht im wesentlichen auf einer Eigenschaft dieser Systeme, die in dem soeben erwähnten einfachsten Falle noch nicht auftritt.

Es kann nämlich $(M_1, \ldots, M_h)$ ein zweites Divisorensystem $(N_1, \ldots, N_g)$ enthalten und doch nicht als Produkt dieses Divisorensystems mit einem dritten $(N'_1, \ldots, N'_g)$ darstellbar sein. Der Begriff des „Enthaltens" ist also um vieles weiter als der der „Teilbarkeit". Wir zeigen dies an einem einfachen Beispiele: Es enthält — wie unmittelbar ersichtlich — (x^2, y^2) das Divisorensystem (x, y). Trotzdem können keine Formen $X_1, \ldots, X_k$ existieren, so daß

$$(x^2, y^2) \simeq (x, y)(X_1, \ldots, X_k)$$

wird.

Das Divisorensystem (x^2, y^2) gestattet, um das Resultat sogleich allgemeiner zu fassen, überhaupt keine „echte" Zerlegung. Ist nämlich

$$(x^2, y^2) \simeq (X_1, \ldots, X_k)(Y_1, \ldots, Y_l),$$

so kann bewiesen werden, daß der eine Faktor mit der Einheit, der andere mit dem Systeme (x^2, y^2) äquivalent ist. Man kann jedenfalls

$$X_i \equiv a_i + b_i x + c_i y + d_i xy, \text{ (mod. } x^2, y^2)$$
$$Y_j \equiv p_j + q_j x + r_j y + s_j xy, \text{ (mod. } x^2, y^2)$$

schreiben. Soll nun der Annahme nach

$$X_i Y_j \equiv 0 \text{ (mod. } x^2, y^2)$$

sein, so muß auch

$$a_i p_j = 0, \ (i = 1, \ldots, k; \ j = 1, \ldots, l),$$

sein, d. h. entweder sämtliche $a_1, \ldots, a_k$ oder aber sämtliche $p_1, \ldots, p_l$ verschwinden. Sind nun z. B. die Größen p nicht sämtlich Null, so müssen wieder die b, c und d sämtlich Null sein, d. h. das Divisorensystem $(X_1, \ldots, X_k)$ enthält (x^2, y^2) und, da auch das Umgekehrte der Fall ist, hat man

$$(X_1, \ldots, X_k) \simeq (x^2, y^2)$$

und also

$$(Y_1, \ldots, Y_k) \simeq 1.$$

Ein Divisorensystem heißt unzerlegbar oder irreduzibel, wenn es keine „echte“ Zerlegung gestattet, d. h. wenn es nur in der Weise als Produkt zweier Faktoren darstellbar ist, daß der eine Faktor dem vorgelegten Systeme, der andere Faktor also — gemäß dem früher Bewiesenen — der Einheit äquivalent ist. Das gegebene Beispiel zeigt aber, daß ein unzerlegbares Divisorensystem trotzdem solche Divisorensysteme enthalten kann, die weder der Einheit noch dem gegebenen Systeme selbst äquivalent sind.

Ein Divisorensystem heißt ein Primsystem*) (Primdivisorensystem, Primmodulsystem), wenn für jedes

*) In der „Festschrift“ gebraucht Kronecker die Ausdrücke irreduzibel und prim noch unterschiedslos für unzerlegbare Systeme. Die hiermit verbundenen Unzukömmlichkeiten führten jedoch dahin, auch hier eine schärfere Unterscheidung zu treffen. (Kronecker, Über einige Anwendungen der Modulsysteme auf elementare algebraische

dieses System enthaltende Produkt auch schon einer der Faktoren das System enthält.

In diesem Sinne ist jede Primgröße, als eingliedriges Divisorensystem aufgefaßt, auch ein Primsystem; ebenso z. B. das Divisorensystem (x, y). Nicht aber trotz seiner Unzerlegbarkeit (x^2, y^2), das in $(x^2, y)(x^2, y)$ enthalten ist, obwohl die Faktoren (x^2, y), wie unmittelbar zu sehen, das Divisorensystem (x^2, y^2) nicht enthalten.

Jedes Primsystem ist irreduzibel, denn die Zerlegung gäbe ein Produkt, in welchem der eine Faktor jenes Primsystem und selbstverständlich das Primsystem auch jenen Faktor enthält; dieser Faktor ist also dem Primsysteme, und also der andere der Einheit äquivalent. Die Umkehrung des Satzes ist, wie dies schon das Beispiel (x^2, y^2) zeigt, nicht richtig.

Ein absolutes Primsystem ist endlich ein solches System, das nur der Einheit oder dem vorgelegten Systeme selbst äquivalente Divisorensysteme enthält*).

Fragen, Journ. f. r. u. a. Math. Bd. 99. pag. 337 = Werke, Bd. III. 1. pag. 158). Die im Texte gegebene Definition des Primsystems stimmt inhaltlich mit der Kroneckerschen überein, ist aber formell einfacher, da sie den Begriff der „Stufe" nicht benutzt.

*) Daß ein so definiertes System $(P_1, P_2, \ldots)$ immer auch ein Primsystem in der früher definierten Bedeutung des Wortes ist, ist wohl einfach zu erschließen, muß aber doch besonders bewiesen werden

Wäre nämlich $(P_1, P_2, \ldots)$ in dem Produkte

$$(F_1, F_2, \ldots)(G_1, G_2, \ldots)$$

enthalten, so müßte es auch in dem Divisorensysteme

$$(F_1, F_2, \ldots, P_1, P_2, \ldots)(G_1, G_2, \ldots)$$

enthalten sein. Nun ist aber der erste dieser Faktoren jedenfalls in $(P_1, P_2, \ldots)$ enthalten, also nach der für dieses System nun statuierten Annahme entweder

$$(F_1, F_2, \ldots, P_1, P_2 \ldots) \simeq (P_1, P_2, \ldots),$$

und dann enthält auch schon $(F_1, F_2, \ldots)$ das System $(P_1, P_2, \ldots)$, oder aber es wäre

$$(F_1, F_2, \ldots, P_1, P_2, \ldots) \simeq 1,$$

und dann würde eben der andere Faktor $(G_1, G_2, \ldots)$ das System $(P_1, P_2, \ldots)$ enthalten.

Im Bereiche der rationalen und ganzen Formen gibt eine Primform $F(x_1, \ldots, x_m)$ wohl, wie schon bemerkt, ein (eingliedriges) Primsystem; dieses ist aber kein absolutes Primsystem, wenn F zumindest eine Unbestimmte x wirklich enthält. Dann kann man nämlich immer rationale und ganze Zahlen $a_1, \ldots, a_m$ so bestimmen, daß $F(a_1, \ldots, a_m)$ weder 0 noch ± 1 wird, also durch eine Primzahl p teilbar wird. Daraus folgt aber:

$$F(x_1, \ldots, x_m) = \sum_{i=1}^{m} G_i(x_i - a_i) + pc,$$

also enthält F das Divisorensystem

$$(x_1 - a_1, \ldots, x_m - a_m, p),$$

das gewiß nicht $\simeq 1$ und auch nicht $\simeq F$ ist. In diesem Falle müßte nämlich p durch F teilbar sein, und das ist unmöglich. Im jenem Falle müßten Formen $H_0, H_1, \ldots, H_m$ existieren, für die

$$\sum_{i=1}^{m} H_i(x_i - a_i) + H_0 p = 1$$

ist, und diese Identität bliebe auch für $x_i = a_i$ richtig und ergäbe dann 1 durch p teilbar, so daß auch diese Annahme sich als absurd erweist.

Dagegen ist $(x_1 - a_1, \ldots, x_m - a_m)$ in jedem einem orthoiden Bereiche (A) entstammenden Formenbereiche

$$[(\mathsf{A}), x_1, \ldots, x_m]$$

ein absolutes Primsystem, wenn $a_1, \ldots, a_m$ Größen des Bereichs (A) bedeuten. Sind nämlich $X_1, \ldots, X_k$ jenem Bereiche entstammende Formen, so kann man jedenfalls

$$X_i \equiv c_i \pmod{x_1 - a_1, \ldots, x_m - a_m}$$

schreiben. Ist dann $(X_1, \ldots, X_k)$ in dem vorgelegten Systeme enthalten, aber diesem nicht äquivalent, so muß mindestens ein c_i von 0 verschieden sein, sonst wäre ja jedes

$$X_i \equiv 0 \pmod{x_1 - a_1, \ldots, x_m - a_m}$$

und es wären die zwei Systeme in der Tat ineinander enthalten, also:

$$(X_1, \ldots, X_k) \simeq (x_1 - a_1, \ldots, x_m - a_m).$$

Ist aber c_i von Null verschieden, so ist weiter

$$c_i \equiv 0 \text{ (mod. } X_i, x_1 - a_1, \ldots, x_m - a_m),$$

also auch

$$c_i \equiv 0 \text{ (mod. } X_1, \ldots, X_k)$$

und, da man in dem orthoiden Bereiche mit c_i dividieren kann,

$$1 \equiv 0 \text{ (mod. } X_1, \ldots, X_k),$$

das heißt:

$$(X_1, \ldots, X_k) \simeq 1.$$

Endliche Divisorenketten.

§ 5. Daß die in der Theorie der algebraischen Größen auftretenden Bereiche diophantische Bereiche sind, wird ganz allgemein durch eine ihnen zukommende Eigenschaft erschlossen, die ausführlich dargelegt werden muß.

Sei A irgend ein (echter oder unechter) holoider Bereich,

$$(S_1), (S_2), \ldots, (S_r), \ldots .$$

eine unbegrenzte Reihe von Divisorensystemen, deren Elemente Größen des Bereichs A sind, und die wir noch der Bedingung unterwerfen, daß jedes Divisorensystem (S_k) im vorher gehenden Systeme (S_{k-1}) enthalten sei.

Eine solche Reihe von Divisorensystemen soll kurz eine Divisorenkette heißen; und es soll schließlich die Divisorenkette $(S_1), (S_2), \ldots, (S_r), \ldots$ endlich genannt werden, wenn man eine positive ganze Zahl r von der Beschaffenheit angeben kann, daß, wenn a irgend eine positive ganze Zahl bedeutet, jedes System $(S_{r+a}) \simeq (S_r)$ ist.

Ist $(S_k) \simeq (G_1, \ldots, G_c)$, so kann man, da (S_{k+1}) der Annahme nach in (S_k) enthalten ist, (S_{k+1}) jedenfalls in der Gestalt

$$(G_1, \ldots, G_c, G_{c+1}, \ldots, G_d)$$

schreiben und dann zwischen (S_k) und (S_{k+1}) die weiteren Systeme

$$((S_k), G_{c+1}), ((S_k), G_{c+1}, G_{c+2}), \ldots, ((S_k), G_{c+1}, \ldots, G_{d-1})$$

„interpolieren". Geschieht dies durchweg, so erhält man, da man vor (S_1) stets $S_0 = 0$ setzen kann, eine Divisorenkette von der speziellen Gestalt

$$F_1, (F_1, F_2), (F_1, F_2, F_3), \ldots$$

die selbstverständlich dann und nur dann endlich ist, wenn dies für die ursprünglich vorgelegte Divisorenkette der Fall ist.

Es gibt Bereiche, in denen jede Divisorenkette endlich ist. Dies ist gewiß der Fall, wenn A ein orthoider Bereich, da ja in diesem jede von 0 verschiedene Größe mit der Einheit äquivalent ist.

Dieselbe Eigenschaft besitzt auch der Bereich [1]. In diesem Falle ist jedes Divisorensystem $(S_k) \simeq d_k$, einer bestimmten positiven ganzen Zahl, und, da (S_k) in (S_{k-1}) enthalten ist, $d_k \leqq d_{k-1}$. Man hat also eine Reihe von niemals zunehmenden positiven ganzen Zahlen

$$d_1, d_2, d_3, \ldots;$$

ist daher d_k die kleinste von ihnen, so wird jedenfalls

$$(S_k) \simeq (S_{k+1}) \simeq (S_{k+2}) \text{ u. s. f.}$$

Man hat nun den fundamentalen Satz:

Ist jede aus den Größen des Bereichs A gebildete Divisorenkette endlich, so ist dasselbe in dem Bereiche der aus A entstammenden Formen von m Unbestimmten $[A, x_1, x_2, \ldots, x_m]$ der Fall.

Da der Satz eben der Annahme nach für $m = 0$ richtig ist, wird der allgemeine Beweis durch den Schluß von $m - 1$ auf m erbracht werden können.

Andrerseits können wir uns im Sinne der vorhergehenden Erörterungen auf jene speziellen Divisorenketten beschränken, in denen

$$(S_k) \simeq (F_1, F_2, \ldots, F_k)$$

ist, und endlich die Formenreihe $F_1, F_2, \ldots$ auf eine gewisse „einfachste“ Gestalt bringen. Es ist nämlich unmittelbar klar, daß man an Stelle von F_r jede Form F_r' setzen kann, für welche

$$F_r' \equiv F_r \pmod{F_1, \ldots, F_{r-1}}$$

ist. Dementsprechend soll an Stelle von F_r jene

$$\text{mod. } (F_1, \ldots, F_{r-1})$$

mit F_r kongruente Form G_r gesetzt werden, die in x_m von möglichst niedrigem Grade ist. Ist $F_r \equiv 0, \pmod{F_1, \ldots, F_{r-1}}$, so kann F_r bei der Bildung der Divisorenkette ganz ausgelassen werden. Die demgemäß in ihrer einfachsten Gestalt geschriebene Divisorenkette

$$\ldots, (G_1, G_2, \ldots, G_k), \ldots \qquad (k = 1, 2, 3, \ldots)$$

muß aber im Endlichen vollständig abbrechen, d. h. es wird von einem bestimmten k ab $G_{k+1} = 0$, $G_{k+2} = 0, \ldots$ sein. Wenn wir diese soeben behauptete Tatsache beweisen, ist damit der zu erschließende Satz in unmittelbare Evidenz gebracht.

Wir zeigen zuerst, daß in der Formenreihe $G_1, G_2, \ldots$ nur eine endliche Anzahl von Formen enthalten ist, die in x_m von einem bestimmten, z. B. n^{ten} Grade sind. Es sei nämlich

$$G_1', G_2', \ldots$$

eine unbegrenzte Reihe solcher Formen, und demgemäß

$$G_r' = \alpha_r x_m^n + \cdots,$$

wo α_r eine aus A entstammende Form der Unbestimmten $x_1, \ldots, x_{m-1}$ ist. Da unser Satz für aus A entstammende Formen von $m - 1$ Unbestimmten richtig ist, wird für die Reihe

$$\alpha_1, \alpha_2, \ldots, \alpha_l, \ldots$$

eine bestimmte positive ganze Zahl existieren, so daß

$$\alpha_{r+a} \equiv 0, \pmod{\alpha_1, \alpha_2, \ldots, \alpha_r},$$

wenn a irgend welche positive ganze Zahl bedeutet. Ist insbesondere

$$\alpha_{r+a} = \beta_{1a}\alpha_1 + \beta_{2a}\alpha_2 + \cdots + \beta_{ra}\alpha_r,$$

so wird

$$G'_{r+a} \equiv G'_{r+a} - \beta_{1a}G'_1 - \beta_{2a}G'_2 - \cdots - \beta_{ra}G'_r \pmod{G'_1, \ldots, G'_r}$$

und, da die rechts stehende Form in x_m den Grad n nicht erreicht, wäre eben G'_{r+a} nicht auf die supponierte „einfachste" Gestalt gebracht. Ist dies geschehn, so muß mithin die Anzahl der in der Reihe $G_1, G_2, \ldots$ vorkommenden Formen, die in x_m vom n^{ten} Grade sind, endlich sein.

Unter denselben Voraussetzungen kann aber der Grad der Formen $G_1, G_2, \ldots$ in x_m eine bestimmte positive ganze Zahl N nicht überschreiten. Wenn dies nicht stattfände, könnte man eine unendliche Reihe von Formen

$$G'_{n_1}, G'_{n_2}, G'_{n_3}, \ldots$$

aus $G_1, G_2, \ldots$ wählen, so daß G'_{n_r} in x_m vom Grade n_r ist, und $n_1, n_2, n_3, \ldots$ eine unendliche Reihe von wachsenden positiven Zahlen wäre. Dabei hätte G'_{n_r} die spezielle Gestalt

$$G'_{n_r} = \alpha_r x_m^{n_r} + \cdots,$$

wo wieder

$$\alpha_1, \alpha_2, \ldots, \alpha_l, \ldots$$

aus A entstammende Formen der $m-1$ Unbestimmten $x_1, x_2, \ldots, x_{m-1}$ sind, und es gibt also wieder jedenfalls eine bestimmte positive ganze Zahl r von der Beschaffenheit, daß

$$\alpha_{r+a} \equiv 0 \pmod{\alpha_1, \alpha_2, \ldots, \alpha_r},$$

wenn a irgend welche positive ganze Zahl bedeutet. Ist insbesondere

$$\alpha_{r+a} = \beta_{1a}\alpha_1 + \beta_{2a}\alpha_2 + \cdots + \beta_{ra}\alpha_r,$$

so wird

$$G'_{n_r+a} \equiv G'_{n_r+a} - \beta_{1a}x_m^{n_r+a-n_1}G'_{n_1} - \cdots + \beta_{ra}x_m^{n_r+a-n_r}G'_{n_r} \pmod{G'_{n_1}, \ldots, G'_{n_r}}$$

und, da die rechts stehende Form den Grad n_{r+a} in x_m nicht erreicht, wäre wieder $G'_{n_{r+a}}$ im Gegensatz zur Annahme nicht auf die „einfachste" Gestalt gebracht. Ist dies geschehn, so gibt es für die Formen nur eine endliche Anzahl von Graden und für jeden Grad nur eine endliche Anzahl von Formen, demnach überhaupt nur eine endliche Anzahl von 0 verschiedener Formen G, und damit ist eben der aufgestellte Satz bewiesen.

Insbesondere ist also jede Divisorenkette in irgend einem orthoiden Formenbereiche, sowie im Bereiche der rationalen und ganzen Formen von beliebig vielen Unbestimmten endlich.

Hieraus folgt unmittelbar der folgende — mit der ganz unwesentlichen Beschränkung auf homogene Formen — zuerst von Hilbert*) aufgestellte Satz:

Aus einer beliebigen Menge von orthoiden oder auch rationalen und ganzen Formen kann man immer eine endliche Anzahl von Formen $F_1, F_2, \ldots, F_k$ so wählen, daß jede andere Form der Menge sich in der Gestalt $\sum_{i=1}^{k} H_i F_i$ darstellen läßt, wo $H_1, H_2, \ldots, H_k$ wieder orthoide, bez. rationale und ganze Formen sind.

Wäre dies nämlich nicht der Fall, so müßte eine unbegrenzte Reihe von Formen

$$F_1, F_2, \ldots, F_r, \ldots$$

existieren, so daß niemals $F_r \equiv 0 \pmod{F_1, \ldots, F_{r-1}}$ wird, und dies ist eben nach dem früher bewiesenen Satze unmöglich.

---

*) „Über die Theorie der algebraischen Formen." (Math. Annalen, XXXVI. Bd. 1890. pag. 473). — Für rationale Formen hat Gordan einen neuen Beweis gegeben. (Göttinger Nachrichten, 1899, pag. 240.) — Die Theorie der Divisorensysteme liefert für den Inhalt des Satzes die obige einfache Fassung und damit auch den hier gegebenen wesentlich kürzeren, durchsichtigen Beweis.

§ 6. Der Satz von der Endlichkeit jeder Divisorenkette in $[(\mathsf{A}), x_1, \ldots, x_m]$ und $[[1], x_1, \ldots, x_m]$ ist, wie besonders betont werden soll, zwar nur durch einen Existenzbeweis begründet, trotzdem aber für unsre Zwecke von fundamentaler Bedeutung.

Aus ihm folgt unmittelbar, daß die Bereiche

$$[(\mathsf{A}), x_1, \ldots, x_m] \text{ und } [[1], x_1, \ldots, x_m]$$

in der Tat diophantische Bereiche sind.

Aus irgend einer Lösung $\xi_1, \xi_2, \ldots, \xi_l$ der diophantischen Gleichung

$$\sum_{i=1}^{l} F_i X_i = 0$$

bilden wir die Form

$$\xi = \xi_1 u_1 + \xi_2 u_2 + \cdots + \xi_l u_l,$$

wo $u_1, u_2, \ldots, u_l$ neue Unbestimmte sind. Wenden wir auf diese Formenmenge den soeben hergeleiteten Satz an, so gibt es eine endliche Anzahl von Formen in dieser Menge

$$\xi^{(j)} = \xi_{1j} u_1 + \cdots + \xi_{lj} u_l \qquad (j = 1, \ldots, k)$$

von der Beschaffenheit, daß jede Form der Menge ξ sich in der Gestalt

$$\xi = \alpha_1 \xi^{(1)} + \cdots + \alpha_k \xi^{(k)}$$

darstellen läßt, wo $\alpha_1, \ldots, \alpha_k$ wieder dem orthoiden Bereiche (A), bez. dem Bereiche $[1]$ entstammende Formen von $x_1, \ldots, x_m, u_1, \ldots, u_l$ sind. Da aber die ξ homogene, lineare Formen der u sind, muß auch schon, wenn α_{j0} das von den u freie Glied der Form α_j bedeutet:

$$\xi = \alpha_{10} \xi^{(1)} + \cdots + \alpha_{k0} \xi^{(k)}$$

und

$$\xi_i = \alpha_{10} \xi_{i1} + \cdots + \alpha_{k0} \xi_{ik} \qquad (i = 1, \ldots, l)$$

sein, w. z. b. w.

Anschließend sei sogleich bemerkt, daß dieselbe Schlußweise wörtlich auch dann gilt, wenn wir es mit der Kongruenz

$$\Sigma F_i X_i \equiv 0, \ (\text{mod. } G_1, G_2, \cdots)$$

zu tun haben, also auch die Lösungen einer solchen Kongruenz eine endliche Schar bilden.

Auch hier haben wir es — wenigstens vorläufig — nur mit einem Existenzbeweise zu tun; und die eigentliche Aufgabe, jene Schar durch eine endliche Anzahl von algebraischen, resp. arithmetischen Operationen wirklich darzustellen, ist damit noch nicht gelöst. Gerade für dieses Problem ist noch das folgende Corollar unsres Hauptsatzes von Wichtigkeit.

§ 7. Es seien

$$F_1, F_2, \ldots, F_k$$

Formen von $x_1, x_2, \ldots, x_m$, deren Koeffizienten dem Bereiche $[(\mathsf{A}), z_1, \ldots, z_r]$, resp. $[[1], z_1, \ldots, z_r]$ angehören. Es sei nun eine beliebige Menge von Formen G des Bereichs

$$[(\mathsf{A}), x_1, \ldots, x_m, z_1, \ldots, z_r], \text{ resp. } [[1], x_1, \ldots, x_m, z_1, \ldots, z_r]$$

gegeben, die sämtlich die Eigenschaft besitzen, daß man zu jedem G eine entsprechende, dem Bereiche $[(\mathsf{A}), z_1, \ldots, z_r]$, resp. $[[1], z_1, \ldots, z_r]$ angehörende, mit G sich ändernde Form H bestimmen kann, für welche

$$HG \equiv 0 \pmod{F_1, \ldots, F_k}$$

wird. Dann gibt es auch eine solche Form K in $[(\mathsf{A}), z_1, \ldots, z_r]$, resp. $[[1], z_1, \ldots, z_r]$, daß für jede Form G jener Menge

$$KG \equiv 0 \pmod{F_1, \ldots, F_k}$$

wird.

Wendet man wieder den Schlußsatz des § 5 auf die Formen G dieser Menge an, so gibt es in ihr eine endliche Anzahl von Formen $G_1, G_2, \ldots, G_s$, so daß für jedes G

$$G = \sum_{i=1}^{s} T_i G_i.$$

wird. Sind also $H_1, \ldots, H_s$ jene Formen, für welche

$$H_i G_i \equiv 0, \pmod{F_1, \ldots, F_k},$$

so wird, wenn man

$$K = H_1 H_2 \ldots H_s$$

setzt, jedenfalls diese Form K die Eigenschaft besitzen, daß für jede Form G der vorgelegten Menge

$$KG \equiv 0 \pmod{F_1, \ldots, F_k}$$

wird.

Insbesondere sei nun F_i eine Form, die $x_1, \ldots, x_{i-1}$ nicht enthält, und wenn man nach Potenzen von x_i ordnet, die Gestalt $Z_i x_i^{n_i} + \cdots$ besitzt, wo Z_i keine der Unbestimmten x enthält; ferner sei Dscr. $\binom{F_1, \ldots, F_k}{x_1, \ldots, x_k}$ von Null verschieden. Dann ist die Bestimmung jener Form K zugleich mit der Auflösung der linearen diophantischen Gleichungen des entsprechenden Bereichs in einer endlichen Anzahl von Schritten gegeben.

Unter der Voraussetzung, daß es eine die x nicht enthaltende Form H gibt, für die

$$HG \equiv 0 \pmod{F_1, \ldots, F_k}$$

wird, muß nämlich G für jedes Wertsystem von $x_1, \ldots, x_k$, das den Gleichungen $F_1 = 0, \ldots, F_k = 0$ genügt, verschwinden. Bei Anwendung des gewöhnlichen Divisionsverfahrens erhält man nun

$$\begin{aligned} G &= F_1 Q_1 + R_1 \\ R_1 &= F_2 Q_2 + R_2 \\ &\cdots\cdots\cdots \end{aligned}$$

und schließlich

$$G = F_1 Q_1 + F_2 Q_2 + \cdots + F_k Q_k + R_{k+1},$$

wo aber R_{k+1} identisch Null sein muß, da es in x_i den Grad n_i nicht erreicht, und doch für die $n_1 \ldots n_k$ verschiedenen Wertsysteme, die den Gleichungen $F_1 = 0, \ldots, F_k = 0$ genügen, verschwindet. Bei dieser Darstellung von G treten als Nenner in $Q_1, \ldots, Q_k$ nur Potenzprodukte der Z_i auf. Setzt man also $Z = Z_1 \ldots Z_k$, so muß es eine bestimmte positive ganze Zahl r geben, so daß auch schon

$$Z^r G \equiv 0 \pmod{F_1, \ldots, F_k}$$

wird, also Z^r den für K festgestellten Bedingungen genügt.

Es kommt also weiter nur auf die Bestimmung dieser Zahl r an, die bei jeder Wahl der Form G genügt. Für diese ergibt sich nun eine notwendige Bedingung, die sodann auch als hinreichend erkannt wird. Wäre nämlich für irgend ein G':

$$Z^{r+1} G' \equiv 0 \pmod{F_1, \ldots, F_k},$$

so muß auch schon die Kongruenz

$$Z^r G' \equiv 0 \pmod{F_1, \ldots, F_k}.$$

gelten. Da aber auch das Umgekehrte stattfindet, müssen sich aus den diophantischen Gleichungen

$$Z^r G = \sum_{i=1}^{k} F_i X_i$$

und

$$Z^{r+1} G' = \sum_{i=1}^{k} F_i Y_i$$

dieselben Lösungen für G, resp. G' ergeben. Ist für die Auflösung dieser Gleichungen nun ein endliches bestimmtes Verfahren bekannt, also

$$G = \sum G_j U_j$$
$$G' = \sum G'_h V_h$$

gegeben, so bedeutet diese Bedingung, daß jedes G_j das Divisorensystem $(\ldots, G'_h, \ldots)$ und jedes G'_h das Divisorensystem $(\ldots, G_j, \ldots)$ enthält, oder also

$$(\ldots, G_j, \ldots) \simeq (\ldots, G'_h, \ldots)$$

sein muß.

Man erhält also, den Zahlen $r = 0, 1, 2, \ldots$ entsprechend, eine Reihe von Divisorensystemen (S_0), (S_1), (S_2), …, deren Äquivalenz wieder nach unserer Annahme in einer endlichen Anzahl von Schritten entschieden werden kann. Nach einer endlichen Anzahl von Versuchen muß man aber zu einer Zahl r gelangen, für die $(S_r) \simeq (S_{r+1})$ ist, und die so bestimmte Zahl genügt den aufgestellten Forderungen.

Würde es nämlich eine Form Γ geben, für die zuerst

$$Z^{r+k} \Gamma \equiv 0 \pmod{F_1, \ldots, F_k}$$

wird, wo k eine positive ganze Zahl ist, so hätte man jedenfalls

$$Z^{r+1}(Z^{k-1}\Gamma) \equiv 0 \pmod{F_1, \ldots, F_k},$$

also, wie eben bewiesen wurde, auch

$$Z^{r+k-1}\Gamma \equiv 0 \pmod{F_1, \ldots, F_k}.$$

Ist nun $k - 1$ nicht Null, so braucht man dieses Verfahren nur genügend oft zu wiederholen, um schließlich

$$Z^r\Gamma \equiv 0 \pmod{F_1, \ldots, F_k}$$

zu erhalten und demnach die Annahme einer solchen Form Γ als unstatthaft zu erweisen.

Sonderung der algebraischen und arithmetischen Probleme.

§ 8. Um für die Theorie der Divisorensysteme und ihre Anwendungen eine feste Grundlage zu schaffen, ist es vor allem notwendig, in jedem gegebenen Falle entscheiden zu können, ob von zwei gegebenen Systemen eines das andere enthält oder nicht. Die Entscheidung der Frage, ob zwei Divisorensysteme äquivalent sind, ist hierin als spezieller Fall enthalten. Nun ist jene Fragestellung unmittelbar auf die Entscheidung zurückzuführen, ob eine gegebene Form F des Bereichs das Divisorensystem $(F_1, \ldots, F_k)$ enthält, d. h. ob eine Lösung der diophantischen Gleichung:

$$F = F_1X_1 + \cdots + F_kX_k$$

existiert, und die vollständige Lösung der zu Beginn dieses Kapitels aufgestellten linearen diophantischen Probleme ergibt daher auch eine vollständige Beantwortung dieser auf die Divisorensysteme bezüglichen Frage.

In der weiteren Darstellung werden die beiden Fälle, wo der zu Grunde liegende Bereich A ein orthoider oder aber ein echter holoider Bereich ist, voneinander zu trennen sein, da sie nicht nur in den anzuwendenden Methoden, sondern auch in der Bedeutung und Interpretation der darzulegenden Tatsachen wesentlich verschiedene Gesichtspunkte bieten.

Insofern der vorgelegte Bereich ein orthoider ist, oder aber, wenn er ein echter holoider Bereich [A] war, wir in der weiteren Behandlung auch die Größen des zugeordneten orthoiden Bereichs (A) zulassen, — was ja darauf hinauskommt, von vornherein den Bereich (A) zu Grunde zu legen — haben wir es mit einer Entwicklung zu tun, die in dem mehrfach erörterten Sinne ausschließlich der Algebra angehört, und bezeichnen daher die Theorie in diesem Falle als algebraische Theorie der linearen diophantischen Systeme.

Im Gegensatze hierzu soll als arithmetische Theorie der linearen diophantischen Systeme der Fall bezeichnet werden, wo wir uns ausschließlich im Bereiche der rationalen und ganzen Formen bewegen. Zu dieser Beschränkung bewegt uns vor allem der Umstand, daß, soweit es sich um die Theorie der algebraischen Größen handelt, und nicht jener einfachere Fall der „algebraischen" Theorie auftritt, wir es ausschließlich mit Problemen zu tun haben, die durch diese „arithmetische" Theorie vollständig gelöst werden*).

Unter einer Lösung der auftretenden Probleme verstehn

---

*) Es mag jedoch sogleich bemerkt werden, daß die hierher gehörigen Ausführungen in Kap. VIII viel weiter reichende Methoden ergeben. Um nur den einfachsten Fall zu erwähnen, übertragen sie sich beinahe wörtlich auf solche vollständige holoide Bereiche, in denen für jede Größe ein endliches Restsystem existiert. Darunter ist Folgendes zu verstehn:

Ist A irgend eine Größe des Bereichs [A], so gibt es immer eine endliche Anzahl von Größen des Bereichs:

$$A_0, A_1, \ldots, A_{k-1},$$

wo die Zahl k durch A vollständig bestimmt ist, so daß jede Größe B des Bereichs [A] mit einer und nur einer der Größen A_i nach dem Modul A kongruent ist.

Eine allgemeine Theorie der holoiden Bereiche kann übrigens im Sinne einer Theorie der algebraischen Größen nicht existieren. Man bedenke, daß z. B. die Gesamtheit der analytischen Funktionen, die durch beständig konvergente Potenzreihen gegeben sind, auch einen vollständigen holoiden Bereich definiert.

wir immer eine solche, die von den gegebenen Größen ausgehend nur eine endliche Anzahl von Operationen erheischt, wobei diese Operationen wieder nur die Anwendung der vier Species und die Bestimmung des größten gemeinschaftlichen Teilers gegebener Größen verlangen. In diesem Sinne wird die vollständige Lösung der auseinandergesetzten linearen diophantischen Probleme und der sich daran knüpfenden Fundamentalaufgaben der allgemeinen Arithmetik (siehe Kap. IX) in diesem Buche meines Wissens zum ersten Male gegeben*).

Algebraische Theorie der linearen diophantischen Systeme.

§ 9. Ist (A) ein orthoider Bereich, so haben wir nach den Auseinandersetzungen in § 1 d. Kap. zuerst die Schar der Lösungen einer einzelnen homogenen linearen Gleichung

$$F_1 X_1 + \cdots + F_k X_k = 0$$

zu bestimmen; damit ist dann die Schar der Lösungen auch für ein System solcher Gleichungen gegeben.

Dabei kann der Schluß von $m-1$ auf m, d. h. der Schluß von $[(A), x_1, \ldots, x_{m-1}]$ auf $[(A), x_1, \ldots, x_m]$ an-

*) An Vorarbeiten sind für die „algebraische" Theorie die sämtlichen auf den Noetherschen Satz (siehe § 12 d. K.) bezüglichen Untersuchungen zu betrachten, die dem Falle von Formen zweier Unbestimmten entsprechen.

Für die „arithmetische" Theorie sind zwei Abhandlungen von Hensel zu nennen: „Über die Zurückführung der Divisorensysteme auf eine reduzierte Form" (Journal f. d. r. u. a. Math. Bd. 118. 1897. u. 119. 1898). In diesen Arbeiten wird für Divisorensysteme, deren Elemente rationale und ganze Formen einer Unbestimmten sind, eine reduzierte Form bestimmt und das speziellere Problem der Äquivalenz zweier solcher Divisorensysteme dahin erledigt, daß eine Äquivalenz dann und nur dann statthat, wenn die entsprechenden reduzierten Systeme dieselben sind.

Mit derselben Frage hat sich auch Hancock beschäftigt (Journal f. d. r. u. a. Math. Bd. 119. 1898. u. Bd. 122. 1900).

gewendet werden. Für den Bereich (A) selbst liegt die Sache sehr einfach. Die vollständige Lösung der Gleichung

$$\gamma_1\xi_1 + \gamma_2\xi_2 + \cdots + \gamma_k\xi_k = 0,$$

in der wenigstens einer der Koeffizienten, z. B. γ_1, von Null verschieden ist, ergibt sich unmittelbar als $k-1$-gliedrige Schar in der Gestalt

$$\xi_1 = -\frac{\gamma_2}{\gamma_1}\mu_2 - \cdots - \frac{\gamma_k}{\gamma_1}\mu_k$$
$$\xi_i = \mu_i \qquad (i = 2, \ldots, k).$$

Da ferner eine Lösung der Gleichung

$$\gamma_1\xi_1 + \gamma_2\xi_2 + \cdots + \gamma_k\xi_k = 1,$$

in welcher z. B. γ_1 von 0 verschieden sein soll, unmittelbar hingeschrieben werden kann:

$$\xi_1 = \frac{1}{\gamma_1},\ \xi_2 = \cdots = \xi_k = 0,$$

sind die beiden Fundamentalprobleme in (A) gelöst, also die Theorie der linearen Systeme für diesen Fall vollständig erledigt.

Wir wollen nun annehmen, daß die vollständige Lösung des homogenen linearen diophantischen Systems in

$$[(A), x_1, \ldots, x_{m-1}]$$

durch ein wohldefiniertes Verfahren erlangt werden kann, wie dies für (A) in der Tat der Fall ist, und unter dieser Annahme ein ebensolches Verfahren für den Bereich

$$[(A), x_1, \ldots, x_m]$$

entwickeln.

Dabei kann vor allem, da eine lineare Transformation an dem Problem nichts ändert, vorausgesetzt werden, daß die Formen $F_1, \ldots, F_k$ durchaus regulär sind. Unter dieser Voraussetzung gestaltet sich die Auflösung der Gleichung

$$F_1X_1 + F_2X_2 + \cdots + F_kX_k = 0, \tag{1}$$

mit welcher auch die Auflösung homogener Systeme erledigt ist, folgendermaßen.

Die unbekannten Formen $X_2, \ldots, X_k$ können, da F_1 regulär ist, jedenfalls in der Gestalt

$$X_i = F_1 \, Y_i + R_i \qquad (i = 2, \cdots, k)$$

geschrieben werden, wo R_i vom höchstens $n_1 - 1^{\text{ten}}$ Grade in x_m, wenn n_1 die Dimension von F_1 ist. Die Gleichung selbst erhält dann die Gestalt

$$F_1(X_1 + F_2 Y_2 + \cdots + F_k Y_k) + F_2 R_2 + \cdots + F_k R_k = 0. \quad (2)$$

Der Grad von $F_2 R_2 + \cdots + F_k R_k$ in x_m ist höchstens gleich der größten der Zahlen $n_i + n_1 - 1$, $(i = 2, \ldots, k)$, wo n_i die Dimension von F_i bedeutet, und daher der Grad von $X_1 + F_2 Y_2 + \cdots + F_k Y_k$ in x_m nicht größer als s, die größte der Zahlen $n_i - 1$. Setzt man also

$$R_i = U_{i0} x_m^{n_1 - 1} + U_{i1} x_m^{n_1 - 2} + \cdots + U_{i, n_1 - 1}$$
$$(i = 2, \ldots, k)$$

$$X_1 + \sum_{i=2}^{k} F_i Y_i = V_0 x_m^s + V_1 x_m^{s-1} + \cdots + V_s,$$

wo die U und V vorläufig unbekannte Formen des Bereichs $[(\mathsf{A}), x_1, \ldots, x_{m-1}]$ bedeuten, in die gegebene Gleichung ein, so erhält man, wenn man die Koeffizienten der einzelnen Potenzen von x_m gleich Null setzt, ein System von hinreichenden und notwendigen Bedingungen für die U und V, die geradezu ein System homogener linearer diophantischer Gleichungen in $[(\mathsf{A}), x_1, \ldots, x_{m-1}]$ darstellen, und deren vollständige Lösung wir der Annahme nach schon bewerkstelligen können. Man erhält mithin die allgemeine Lösung unsres Systems (2) in der Gestalt

$$R_i = \sum_{j=1}^{l} G_{ji} W_j \qquad (i = 2, \ldots, k)$$

$$X_1 + \sum_{i=2}^{k} F_i Y_i = \sum_{j=1}^{l} H_j W_j$$

und also auch die allgemeine Lösung der Gleichung (1):

$$X_1 = -\sum_{i=2}^{k} F_i Y_i + \sum_{j=1}^{l} H_j W_j$$

$$X_i = F_1 Y_i + \sum_{j=1}^{l} G_{ji} W_j,$$

wo H_j, G_{ji} gegebene, Y_i, W_j beliebige Formen bedeuten, demnach in der Gestalt einer höchstens $k + l - 1$-gliedrigen Schar.

Das zweite Fundamentalproblem, zu entscheiden, ob die diophantische Gleichung

$$F_1 X_1 + \cdots + F_k X_k = 1$$

überhaupt Lösungen besitzt, und wenn dies der Fall ist, eine solche zu bestimmen, kann (auch dann, wenn rechts statt der Eins eine beliebige Form F steht) nach der soeben auseinandergesetzten Methode wieder auf den Bereich $[(A), x_1, \ldots, x_{m-1}]$ reduziert werden, ist aber auch durch die Auseinandersetzungen der allgemeinen Eliminationstheorie (Kap. V. § 4, 5) schon vollständig erledigt. Diese wohl nicht elementare, aber gerade, weil sie tiefer liegt, an sich wichtige Methode kann in einigen Zeilen auseinandergesetzt werden.

Ist die Gesamtresolvente des Gleichungssystems

$$F_i = 0 \qquad (i = 1, \ldots, k)$$

im Sinne der Äquivalenz von 1 verschieden, so existiert ein Wurzelsystem der Gleichungen $F_i = 0$. Dann ist eine Lösung jener diophantischen Gleichung unmöglich; denn für solche Formen X_i, die jener diophantischen Gleichung genügen, würde diese eine Identität, welche auch dann gültig bleiben müßte, wenn für die x_i jenes Wurzelsystem gesetzt wird; dies ergäbe aber $0 = 1$.

Ist die Gesamtresolvente des Gleichungssystems der Einheit äquivalent, so ergibt sich für die Resolventenform nach den in Kap. III. § 18 beschriebenen Operationen geradezu eine Identität.

$$1 = \sum_{i=1}^{k} G_i F_i,$$

d. h. eine Lösung der vorgelegten diophantischen Gleichung.

Die Divisorensysteme der Hauptklasse

(deren Elemente einem orthoiden Bereiche entstammende Formen sind).

§ 10. Für solche Divisorensysteme $(F_1, F_2, \ldots, F_k)$, deren Elemente einem orthoiden Bereiche entstammende Formen sind, soll die Stufenzahl des Gleichungssystems $F_j = 0$ oder der durch diese Gleichungen definierten Mannigfaltigkeit auch als Stufenzahl des Divisorensystems bezeichnet werden. Äquivalente Divisorensysteme sind demnach von derselben Stufe, und die Stufenzahl ändert sich auch dann nicht, wenn das Divisorensystem durch irgend eine (homogene) lineare Transformation der Unbestimmten x in ein Divisorensystem übergeführt wird, dessen Elemente nun Formen der Unbestimmten z sind.

Für die in Betracht gezogenen diophantischen Probleme wird durch eine solche lineare Transformation an der Fragestellung nichts geändert, und wir wollen demnach von vornherein auf das Divisorensystem, d. h. auf sämtliche Elemente desselben, wo dies notwendig erscheint, eine „allgemeine" Transformation ausgeübt denken. Darunter ist eine solche zu verstehn, für welche die Koeffizienten der Transformation gewissen bestimmten algebraischen Gleichungen nicht genügen.

Ein Divisorensystem soll als der Hauptklasse angehörig bezeichnet werden*), wenn es einem solchen Systeme $(F_1, F_2, \ldots, F_k)$ äquivalent ist, für welches $(F_i, \ldots, F_k)$ genau von der $k - i + 1^{\text{ten}}$ Stufe ist. Wir wollen von jetzt an ein Divisorensystem der Hauptklasse schon als in dieser Gestalt gegeben annehmen. Dabei kann $k \leq m$ angenommen werden; der Stufenzahl $m + 1$ entsprechen nämlich nur der Einheit äquivalente Divisorensysteme, deren Eigenschaften mit der soeben ausgesprochenen erschöpft sind.

---

*) Man zeigt übrigens leicht, daß jedes k-gliedrige Divisorensystem k^{ter} Stufe im angegebenen Sinne der Hauptklasse angehört.

Eine Fundamentaleigenschaft eines solchen k-gliedrigen Divisorensystems k^{ter} Stufe kann dahin ausgesprochen werden, daß das Gleichungssystem

$$F_j = 0 \qquad (j = 1, \ldots, k),$$

in dem man $x_1, \ldots, x_k$ als Unbekannte zu betrachten hat, während die Koeffizienten dem orthoiden Bereiche (A) entstammende Formen $x_{k+1}, \ldots, x_m$ sind, eine endliche (von 0 verschiedene) Anzahl von Wurzelsystemen besitzt. (Ist $k = m$, so enthalten die Koeffizienten keine Unbestimmte.)

Wie aus der Definition der Hauptklasse unmittelbar ersichtlich, gehört mit $(F_1, F_2, \ldots, F_k)$ auch $(F_i, \ldots, F_k)$ immer der Hauptklasse an. Es wird damit die Tatsache ausgesprochen, daß das Gleichungssystem $F_i = 0, \ldots, F_k = 0$ eine endliche und von 0 verschiedene Anzahl von Wurzelsystemen besitzt, wenn $k - i + 1$ der Größen x als Unbekannte, und $m - k + i - 1$ davon als in den Koeffizienten auftretende Unbestimmte aufgefaßt werden. Wegen der auf die F ausgeübten allgemeinen linearen Transformation ist es dabei völlig gleichgültig, wie diese Trennung der x vorgenommen wird.

Bildet man jetzt die Gesamtresolvente des Systems $F_1 = 0, \ldots, F_k = 0$, indem man zu diesem Zweck die neue Unbekannte

$$z_1 = t_{11}x_1 + t_{12}x_2 + \cdots + t_{1m}x_m$$

einführt, so wird diese $R_1(z_1, x_{k+1}, \ldots, x_m) = 0$, und es ist

$$R_1\left(\sum_{i=1}^{m} t_{1i}x_i, x_{k+1}, \ldots, x_m\right) = \sum_{j=1}^{k} \lambda_{1j}F_j.$$

Dabei ist nach den Entwicklungen der allgemeinen Eliminationstheorie der Koeffizient der höchsten Potenz von z_1 in R_1 eine von den x unabhängige Größe, und es muß R_1 eine wirkliche Form von z_1 sein. Zum Vergleiche mit Kap. V. § 2. 3 sei noch bemerkt, daß jetzt der bessern Übersicht wegen die Bedeutung von x_k und x_m vertauscht wurde.

Wir wissen weiter, daß, wenn man $R_1 = 0$ als Komplex von Gleichungen auffaßt, d. h. die Koeffizienten, die neben den verschiedenen Potenzprodukten der t_{1i} auftreten, gesondert gleich Null setzt, die Systeme $R_1 = 0$ und $F_j = 0$ dieselben Wurzelsysteme besitzen.

Diese Tatsache kann auch so interpretiert werden, daß die Gleichungssysteme

$$F_1 = 0,\ F_2 = 0,\ \ldots,\ F_k = 0$$

und

$$R_1\left(\sum_{i=1}^{m} t_{1i}x_i,\ x_{k+1},\ \ldots,\ x_m\right) = 0,\ F_2 = 0, \ldots, F_k = 0,$$

insofern man sich auf von den t unabhängige Größen beschränkt, dieselben Wurzelsysteme besitzen.

Wendet man nun auf dieses letztere Gleichungssystem dieselben Operationen an und bildet insbesondere die Gesamtresolvente, indem man die neue Unbekannte

$$z_2 = t_{21}x_1 + t_{22}x_2 + \cdots + t_{2m}x_m,$$

einführt, so erhält man

$$R_2\left(\sum_{i=1}^{m} t_{2i}x_i,\ x_{k+1},\ \ldots,\ x_m\right) = \lambda_{21}R_1 + \sum_{j=2}^{k} \lambda_{2j}F_j,$$

wo $R_2(z_2, x_{k+1}, \ldots, x_m)$, da das jetzt betrachtete System, wie nachträglich bewiesen werden soll, wieder von der k^{ten} Stufe ist, in Bezug auf z_2 genau dieselben Eigenschaften besitzt, wie R_1 in Bezug auf z_1. Die Gleichung $R_2 = 0$, ähnlich wie früher aufgefaßt, ergibt wieder die Wurzelsysteme von $F_1 = 0, \ldots, F_k = 0$, und nur diese, wenn man sich auf von den t unabhängige Größen beschränkt.

In dieser Weise fortfahrend, bilden wir die Formenreihe

. . . . . .

$$R_\mu\left(\sum_{i=1}^{m} t_{\mu i}x_i,\ x_{k+1},\ \ldots,\ x_m\right) = \sum_{\varrho=1}^{\mu-1} \lambda_{\mu\varrho}R_\varrho + \sum_{j=\mu}^{k} \lambda_{\mu j}F_j,$$

. . . . . .

$$R_k\left(\sum_{i=1}^{m} t_{ki}x_i,\ x_{k+1},\ \ldots,\ x_m\right) = \sum_{\varrho=1}^{k-1} \lambda_{k\varrho}R_\varrho + \lambda_{kk}F_k.$$

Wir können und wollen für die Größen $t_{\mu i}$ solche spezielle (auch rationale und ganze) Werte setzen, für welche den angeführten Eigenschaften der $R_1, R_2, \ldots, R_k$ kein Abbruch geschieht, und auch die Determinante $|t_{\mu i}|_{(\mu, i=1,\ldots,k)}$ von 0 verschieden ist. Faßt man nun

$$z_\mu = \sum_{i=1}^{m} t_{\mu i} x_i \qquad (\mu = 1, \ldots, k)$$

als lineare Transformation auf und schreibt schließlich wieder x statt z, so hat man nach einer passenden linearen Transformation des vorgelegten Divisorensystems die Formenreihe

$$R_\mu(x_\mu, x_{k+1}, \ldots, x_m) = \sum_{\varrho=1}^{\mu-1} \lambda_{\mu\varrho} R_\varrho + \sum_{j=\mu}^{k} \lambda_{\mu j} F_j \qquad (\mathrm{R}_\mu)$$
$$(\mu = 1, \ldots, k)$$

bestimmt, wo die R_μ durchweg wirkliche Formen von x_μ sind, in denen der Koeffizient der höchsten Potenz von x_μ eine von den übrigen x unabhängige Größe ist. Die F_j können als regulär angenommen werden, da man zuerst eine dies bewerkstelligende Transformation anwenden und die weiteren dann immer so wählen kann, daß diese Eigenschaft erhalten bleibt.

Die Existenz der Formenreihe R_μ hängt aber noch von der bisher nicht bewiesenen Annahme ab, daß jedes Gleichungssystem

$$R_1 = 0, \ldots, R_{i-1} = 0, F_i = 0, \ldots, F_k = 0,$$

das man jetzt als aus k Gleichungen bestehendes System mit von den t abhängigen Koeffizienten aufzufassen hat, von der k^{ten} Stufe ist. Die Stufenzahl des Systems $F_i = 0, \ldots, F_k = 0$ ist der Annahme nach $k - i + 1$ und ändert sich nicht, wenn man die Formen F als dem orthoiden Bereiche $((\mathsf{A}), t_{11}, \ldots)$ entstammend auffaßt; weil sich hierbei an der Bildung der Gesamtresolvente nichts ändert. Unser Gleichungssystem ist auch schon „von Zufälligkeiten befreit“; denn dies geschieht durch eine homogene lineare Transformation der Unbekannten mit rationalen und ganzen Koeffizienten, und es kann demnach

angenommen werden, daß diese Transformation schon ursprünglich an den F ausgeübt wurde. Ebensowenig ändert sich der „allgemeine“ Charakter des Gleichungssystems, wenn wir mittels der Gleichungen

$$z_\mu = \sum_{i=1}^{m} t_{\mu i} x_i, \qquad (\mu = 1, 2, \ldots, i-1)$$

statt $x_1, \ldots, x_{i-1}$ die neuen Unbekannten $z_1, \ldots, z_{i-1}$ einführen. Dann entspricht aber jedem Wertsysteme von $x_{k+1}, \ldots, x_m$ aus den Gleichungen $R_\mu = 0$ eine endliche und von Null verschiedene Anzahl von Werten für $z_1, \ldots, z_{i-1}$, und aus den Gleichungen $F_i = 0, \ldots, F_k = 0$ weiter eine ebensolche Anzahl von Werten für $x_i, \ldots, x_k$, was eben zu beweisen war.

Sind die der Annahme nach in endlicher und von 0 verschiedener Anzahl vorhandenen Wurzelsysteme von $F_j = 0$, wo $x_1, \ldots, x_k$ als Unbekannte, $x_{k+1}, \ldots, x_m$ als in den Koeffizienten auftretende Unbestimmte zu fassen sind,

$$\xi_{1\nu}, \xi_{2\nu}, \ldots, \xi_{k\nu}, \qquad (\nu = 1, 2, \ldots, r)$$

so genügen diese Wurzelsysteme auch der Gleichung $R_\mu = 0$, d. h. man kann

$$R_\mu = A_\mu \prod_{\nu=1}^{s} (x_\mu - \xi_{\mu\nu})^{c_{\mu\nu}} \qquad (r \leqq s)$$

setzen, wo A_μ dem ursprünglichen orthoiden Bereiche angehört und also auch gleich Eins angenommen werden kann. Es beginnt demnach die Entwicklung von R_μ nach Potenzen von $x_\mu - \xi_{\mu\nu}$ mit der $c_{\mu\nu}^{\text{ten}}$ Potenz, oder, wie wir uns auch ausdrücken können, da die übrigen Glieder fehlen, die Entwicklung von R_μ nach den Potenzprodukten der $x_1 - \xi_{1\nu}, x_2 - \xi_{2\nu}, \ldots, x_k - \xi_{k\nu}$, mit den Gliedern $c_{\mu\nu}^{\text{ter}}$ Dimension als denjenigen niedrigster Dimension.

§ 11. Die Frage, ob ein Divisorensystem oder, was auf dasselbe hinauskommt, eine einzelne Form des Divisorensystems $(F_1, \ldots, F_k)$ enthält, kann durch Auflösung der entsprechenden linearen diophantischen Gleichung in einer endlichen Anzahl

von Schritten erledigt werden. Diese Auflösung leidet aber an dem Übelstande, daß sie für jede Form Φ besonders vorgenommen werden muß. Dem gegenüber ist es von fundamentaler Wichtigkeit, eine endliche Reihe von festen Operationen anzugeben, die, an der Form Φ vorgenommen, darüber entscheidet, ob eine beliebige Form Φ das gegebene Divisorensystem $(F_1, \ldots, F_k)$ enthält. Dies soll für Divisorensysteme der Hauptklasse vollständig durchgeführt werden.

Für der Hauptklasse angehörige Divisorensysteme erster Stufe, d. h. für einzelne Formen, ist dies nichts anderes als das gewöhnliche Teilbarkeitsproblem, und der allgemeine Fall wird geradezu auf dieses zurückgeführt werden können, und zwar durch den folgenden grundlegenden Satz:

Um zu entscheiden, ob eine beliebige Form das gegebene Divisorensystem der Hauptklasse $(F_1, \ldots, F_k)$ enthält, bestimme man k Formen

$$R_\mu(x_\mu, x_{k+1}, \ldots, x_m), \quad (\mu = 1, \ldots, k),$$

ferner Formen $\lambda_{\mu\nu}$, die den Relationen

$$R_\mu(x_\mu, x_{k+1}, \ldots, x_m) = \sum_{\nu=1}^{\mu-1} \lambda_{\mu\nu} R_\nu + \sum_{j=\mu}^{k} \lambda_{\mu j} F_j \qquad (\mathrm{R}_\mu)$$

genügen, wo noch $R_\mu = A_\mu x_\mu^{k_\mu} + \ldots$, A_μ die x nicht enthält und $k_\mu \geqq 1$ ist. Man hat dann und nur dann

$$\Phi \equiv 0 \pmod{F_1, \ldots, F_k}, \qquad (\mathrm{C})$$

wenn

$$\lambda_{11}\lambda_{22}\ldots\lambda_{kk}\Phi \equiv 0 \pmod{R_1, \ldots, R_k} \qquad (\mathrm{K})$$

ist, und erhält aus den Darstellungen der letzteren Form

$$\lambda_{11}\ldots\lambda_{kk}\Phi = \sum_{i=1}^{k} K_i R_i$$

auch die Darstellungen von Φ

$$\Phi = \sum_{i=1}^{m} H_i F_i.$$

Daß eine solche Reihe von Formen R und λ nach einer eventuell an dem Divisorensystem auszuübenden linearen Trans-

formation immer bestimmt werden kann, ist eben im vorhergehenden Paragraphen bewiesen worden.

Bevor wir auf den Beweis des ausgesprochenen Satzes eingehn, sollen noch einige auf ihn bezügliche Vorbemerkungen eingeschaltet werden.

Ob die durch (K) ausgedrückte Bedingung erfüllt ist, kann durch das gewöhnliche Divisionsverfahren ermittelt werden. Ist nämlich

$$\Psi = \sum_{i=1}^{k} K_i R_i,$$

so kann man

$$K_i = M_i R_1 + N_i, \qquad (i = 2, \ldots, k)$$

setzen; dann erhält Ψ die Gestalt:

$$\Psi = (K_1 + M_2 R_2 + \cdots + M_k R_k) R_1 + \sum_{i=2}^{k} N_i R_i,$$

und der Koeffizient von R_1 ist der „Quotient", $\sum_{i=2}^{k} N_i R_i$ der „Rest", der bei der „Division" von Ψ durch R_1 auftritt. Man erhält in dieser Weise durch wiederholte Anwendung des Divisionsverfahrens

$$\Psi = \sum_{i=1}^{k} Q_i R_i,$$

wo der Grad von Q_i in Bezug auf die Unbestimmten $x_1, \ldots, x_{i-1}$ kleiner als der Grad von $R_1, \ldots, R_{i-1}$ in Bezug auf die entsprechende Unbestimmte ist.

Die Bedingung $\Psi \equiv 0 \pmod{R_1, \ldots, R_k}$ ist also dann und nur dann erfüllt, wenn man bei wiederholter Anwendung des gewöhnlichen Divisionsverfahrens nach der k^{ten} Division zum Reste „Null" gelangt, und man hat in diesem Falle zugleich die Darstellung $\Psi = \sum_{i=1}^{k} Q_i R_i$ gefunden.

Ist demnach $G(x_{k+1}, \ldots, x_m)$ eine Form, in der die Unbestimmten $x_1, \ldots, x_k$ nicht vorkommen, so ist mit $G\Psi \equiv 0 \pmod{R_1, \ldots, R_k}$ auch $\Psi \equiv 0 \pmod{R_1, \ldots, R_k}$, da bei Anwendung jenes Divisionsverfahrens alle Q_i der Reihe nach durch G teilbar sind.

Daraus folgt aber, daß, wenn man den zu beweisenden Satz vorläufig als richtig annimmt, mit $G(x_{k+1}, \ldots, x_m)\,\Phi \equiv 0 \pmod{F_1, \ldots, F_k}$ immer auch $\Phi \equiv 0 \pmod{F_1, \ldots, F_k}$ ist.

Nach der vorstehenden Bemerkung folgt nämlich aus

$$\lambda_{11} \ldots \lambda_{kk}\, G\Phi \equiv 0 \pmod{R_1, \ldots, R_k}$$

immer auch

$$\lambda_{11} \ldots \lambda_{kk}\, \Phi \equiv 0 \pmod{R_1, \ldots, R_k}.$$

Daß endlich der zu beweisende Satz für $k = 1$ richtig ist, sieht man ganz unmittelbar. In diesem Falle hat man

$$R_1 = \lambda_{11} F_1,$$

und der Satz drückt nur die triviale Tatsache aus, daß die Teilbarkeit von $\lambda_{11}\Phi$ durch $R_1 = \lambda_{11} F_1$ immer zugleich mit der Teilbarkeit von Φ durch F_1 stattfindet.

Für den allgemeinen Beweis des ausgesprochenen Satzes wird demnach die vollständige Induktion eintreten können. Diese soll nun im folgenden so ausgeführt werden, daß wir die Richtigkeit des Satzes für $k-1$-gliedrige Divisoren der Hauptklasse voraussetzen und ihn unter dieser Annahme für k-gliedrige Divisoren der Hauptklasse als gültig erweisen.

Dies geschieht in einfachster Weise. Aus

$$\Phi = \sum_{i=1}^{k} H_i F_i$$

folgt

$$\lambda_{11}\Phi = H_1 \lambda_{11} F_1 + \sum_{i=2}^{k} H_i' F_i$$

oder auch wegen

$$R_1 = \lambda_{11} F_1 + \lambda_{12} F_2 + \cdots + \lambda_{1k} F_k$$

weiter

$$\lambda_{11}\Phi = H_1'' R_1 + \sum_{i=2}^{k} H_i'' F_i.$$

Umgekehrt ergibt aber die letzte Relation

$$\lambda_{11}\Phi = H_1'' \lambda_{11} F_1 + \sum_{i=2}^{k} H_i''' F_i$$

oder

$$\lambda_{11}(\Phi - H_1'' F_1) = \sum_{i=2}^{k} H_i''' F_i,$$

also auch

$$\lambda_{11} F_1 (\Phi - H_1'' F_1) = \sum_{i=2}^{k} H_i''' F_1 F_i$$

und

$$R_1(\Phi - H_1'' F_1) = \sum_{i=2}^{k} H_i' F_i.$$

Nun ist $(F_2, \ldots, F_k)$ ein $k-1$-gliedriges Divisorensystem der Hauptklasse, in dem, wenn nur die zu Beginn gewählte lineare Transformation passend bestimmt war, $x_2, \ldots, x_k$ jene Unbestimmten sind, nach denen die weiteren Operationen erfolgen. Diese sind aber in R_1 nicht enthalten, und man erhält demnach

$$\Phi - H_1'' F_1 = \sum_{i=2}^{k} H_i F_i.$$

Es sind folglich die Kongruenzen

$$\Phi \equiv 0 \pmod{F_1, \ldots, F_k}$$
$$\lambda_{11}\Phi \equiv 0 \pmod{R_1, F_2, \ldots, F_k}$$

zu gleicher Zeit gültig oder ungültig, und aus der entsprechenden Darstellung von $\lambda_{11}\Phi$ ergibt sich durch bekannte Operationen diejenige von Φ.

Die Anwendung desselben Verfahrens auf das Divisorensystem $(R_1, F_2, \ldots, F_k)$ führt ebenso zur Kongruenz

$$\lambda_{11}\lambda_{22}\Phi \equiv 0 \pmod{R_1, R_2, F_3, \ldots, F_k}$$

und so fort, bis man schließlich zur Kongruenz

$$\lambda_{11} \ldots \lambda_{kk}\Phi \equiv 0 \pmod{R_1, \ldots, R_k}$$

gelangt, womit der ausgesprochene Satz vollständig bewiesen ist.

Der verallgemeinerte Noethersche Satz.

§ 12. Es seien die Elemente des k-gliedrigen Divisorensystems der Hauptklasse $(F_1, \ldots, F_k)$ solche Formen, die dem orthoiden Bereiche (A) entstammen

und als solche nur die k weiteren Unbestimmten $x_1, \ldots, x_k$ enthalten; dem Früheren gegenüber ist also $m = k$. Die notwendige und hinreichende Bedingung dafür, daß Φ dieses Divisorensystem enthalte, die wir noch, $\Delta = \lambda_{11} \ldots \lambda_{kk}$ gesetzt, kürzer

$$\Delta\Phi \equiv 0 \pmod{R_1, \ldots, R_k} \qquad \text{(K)}$$

schreiben, läßt sich nun in eine Reihe von Kongruenzbedingungen spalten, die sich auf die einzelnen Wurzelsysteme des Gleichungssystems $F_1 = 0, \ldots, F_k = 0$ beziehen, wenn man zugleich statt (A) den aus (A) entstammenden, durch das Gleichungssystem $F_j = 0$ definierten Gattungsbereich zu Grunde legt.

Wir definierten in § 10 d. Kap.

$$R_\mu = (x_\mu - \xi_{\mu 1})^{c_{\mu 1}} \ldots (x_\mu - \xi_{\mu \nu})^{c_{\mu \nu}} \ldots,$$

wo $\xi_{\mu 1}, \ldots, \xi_{\mu \nu}, \ldots$ die Reihe der Wurzeln von $R_\mu = 0$ bedeutet, also jedenfalls die in den Wurzelsystemen von $F_j = 0$ auftretenden verschiedenen Werte der Unbekannten x_μ enthalten. Man hat demnach

$$\left((x_\mu - \xi_{\mu \nu})^{c_{\mu \nu}}, (x_\mu - \xi_{\mu \nu'})^{c_{\mu \nu'}}\right) \simeq 1,$$

wenn $\nu \neq \nu'$ ist; dabei ist zu beachten, daß nach der auf die F angewandten allgemeinen linearen Transformation in verschiedenen Wurzelsystemen auch alle einzelnen Unbekannten verschiedene Werte annehmen.

Das Divisorensystem $(R_1, \ldots, R_k)$ zerlegt sich aber (nach § 3), wenn jener Gattungsbereich zu Grunde gelegt ist, in ein Produkt von Faktoren, die die Gestalt

$$\left((x_1 - \xi_{1 \nu_1})^{c_{1 \nu_1}}, (x_2 - \xi_{2 \nu_2})^{c_{2 \nu_2}}, \ldots, (x_k - \xi_{k \nu_k})^{c_{k \nu_k}}\right)$$

besitzen, wo $\xi_{1 \nu_1}, \ldots, \xi_{k \nu_k}$ einzeln und voneinander unabhängig unter andern auch die in den Wurzelsystemen von $F_j = 0$ auftretenden Werte der Unbekannten $x_1, \ldots, x_k$ durchlaufen. Bezeichnet man diese Faktoren kurz mit $\{\nu_1, \ldots, \nu_k\}$, so werden in zwei verschiedenen Faktoren $\{\nu_1, \ldots, \nu_k\}$ und $\{\nu_1', \ldots, \nu_k'\}$ die Größen $\xi_{1 \nu_1}, \ldots, \xi_{k \nu_k}$ und $\xi_{1 \nu_1'}, \ldots, \xi_{1 \nu_k'}$ nicht sämtlich gleich

sein; die verschiedenen Faktoren sind also relativ prim, und die Kongruenz (K) wird daher nach § 3 d. Kap. durch das System von Kongruenzen

$$\Delta\Phi \equiv 0 \pmod{\{\nu_1, \ldots \nu_k\}}, \qquad (K'_\nu)$$

die mit (K) gleichbedeutend sind, vollständig ersetzt.

Dabei sind zwei Fälle möglich; die Größen $\xi_{1\nu_1}, \ldots, \xi_{k\nu_k}$ bilden ein Wurzelsystem von $F_j = 0$, oder es ist dies nicht der Fall. Die dem letzteren Falle entsprechenden Kongruenzen sind aber identisch erfüllt und können ganz weggelassen werden; denn es ist, wie wir leicht nachweisen können

$$\Delta \equiv 0 \pmod{\{\nu_1, \ldots, \nu_k\}}.$$

Man hat nämlich jedenfalls:

$$\Delta F_j \equiv 0 \pmod{\{\nu_1, \ldots, \nu_k\}},$$

und, da wenigstens ein F_j für die Werte $x_1 = \xi_{1\nu_1}, \ldots$ $x_k = \xi_{k\nu_k}$ nicht verschwindet, auch

$$(F_j, \{\nu_1, \ldots, \nu_k\}) \simeq 1.$$

Dann enthält aber ΔF_j nicht nur F_j und $\{\nu_1, \ldots, \nu_k\}$, sondern nach § 3 auch das Produkt dieser beiden Divisorensysteme; also ist in der Tat:

$$\Delta \equiv 0 \pmod{\{\nu_1, \ldots, \nu_k\}}.$$

Bezeichnet man demnach die Wurzelsysteme von $F_1 = 0$, $\ldots$, $F_k = 0$ wieder mit

$$\xi_{1\nu}, \xi_{2\nu}, \ldots, \xi_{k\nu}, \qquad (\nu = 1, \ldots, r)$$

so tritt an Stelle der Kongruenz (K) das System von Kongruenzen:

$$\Delta\Phi \equiv 0, \pmod{(x_1 - \xi_{1\nu})^{c_{1\nu}}, (x_2 - \xi_{2\nu})^{c_{2\nu}}, \cdots, (x_k - \xi_{k\nu})^{c_{k\nu}}} \qquad (K_\nu)$$
$$(\nu = 1, \ldots, r).$$

Allerdings sichert dieses System von Kongruenzen, dem Wortlaute des Beweises nach, nur eine solche Darstellung von $\Phi = \sum_{i=1}^{k} H_i F_i$, wo die Koeffizienten der Formen H_i einem

aus (A) entstammenden Gattungsbereiche angehören. Daraus folgt aber auch immer eine Darstellung von Φ, in welcher die H_i dem Bereiche (A) entstammende Formen sind*).

Die Bedingungen (K) und (K_ν) ersetzen sich demnach gegenseitig.

Die Bedingungen (K_ν) lassen sich nun auf eine Gestalt bringen, die für die weiteren Folgerungen von grundlegender Bedeutung ist:

Es seien $\xi_{1\nu}, \ldots, \xi_{k\nu}$, $(\nu = 1, \ldots, r)$ die sämtlichen verschiedenen Wurzelsysteme des Gleichungssystems $F_j = 0$, und $c_{i\nu}$ die Multiplizität der Wurzel $\xi_{i\nu}$ in $R_i = 0$; dann läßt sich die notwendige und hinreichende Bedingung dafür, daß Φ das k-gliedrige Divisorensystem der Hauptklasse $(F_1, \ldots, F_k)$ enthalte, auch folgendermaßen aussprechen: Es müssen sich Formen $K_{\nu 1}, \ldots, K_{\nu k}$ von der Beschaffenheit bestimmen lassen, daß in der Entwicklung von

$$\Delta\Phi - \sum_{i=1}^{k} K_{\nu i} R_i$$

nach den Potenzprodukten der $x_1 - \xi_{1\nu}, \ldots, x_k - \xi_{k\nu}$ keine Glieder vorkommen, deren Dimension $\leqq \sum_{i=1}^{k} c_{i\nu} - k$ ist.

Die ausgesprochene Bedingung ist jedenfalls notwendig; denn es gibt, wenn Φ die geforderte Eigenschaft besitzt, auch Formen K_i für welche jener Ausdruck identisch Null wird.

Daß sie auch hinreichend ist, ersieht man daraus, daß

*) Ist nämlich $\Delta\Phi \equiv 0 \pmod{R_1, \ldots, R_k}$, so kann eine Darstellung

$$\Delta\Phi = \sum_{i=1}^{k} K_i R_i$$

auch immer durch das gewöhnliche Divisionsverfahren, d. h. durch rationale Operationen erhalten werden; und ebenso gelangt man wieder durch rationale Operationen von dieser zur Darstellung

$$\Phi = \sum_{i=1}^{k} H_i F_i$$

zurück.

dann in der Entwicklung von $\Delta\Phi - \sum_{i=1}^{k} K_{\nu i} R_i$ jedes Glied mindestens einen Faktor $x_i - \xi_{i\nu}$ mit dem Exponenten $c_{i\nu}$ enthalten muß. Wäre für jeden solchen Faktor der Exponent $\leqq c_{i\nu} - 1$, so wäre die Dimension des betreffenden Gliedes eben $\leqq \sum_{i=1}^{k} c_{i\nu} - k$. Es ist demnach

$$\Delta\Phi - \sum_{i=1}^{k} K_{\nu i} R_i \equiv 0 \ (\text{mod. } (x_1 - \xi_{1\nu})^{c_{1\nu}}, \cdots, (x_k - \xi_{k\nu})^{c_{k\nu}})$$

und also auch

$$\Delta\Phi \equiv 0 \ (\text{mod. } (x_1 - \xi_{1\nu})^{c_{1\nu}}, \cdots, (x_k - \xi_{k\nu})^{c_{k\nu}}).$$

§ 13. Auf Grundlage dieser Entwicklungen erhalten wir endlich den „verallgemeinerten Noetherschen Satz“*), der für die Theorie der algebraischen Größen, insbesondere eine Reihe von Anwendungen derselben grundlegende Bedeutung besitzt:

Es seien $\xi_{1\nu}, \ldots, \xi_{k\nu}$, $(\nu = 1, \ldots, r)$ die sämtlichen verschiedenen Wurzelsysteme des Gleichungssystems $F_1 = 0, \ldots, F_k = 0$, in dem wir $x_1, \ldots, x_k$ als Unbekannte auffassen; es seien ferner in λ_{jj}, wenn diese Formen nach Potenzprodukten von $x_1 - \xi_{1\nu}, \ldots, x_k - \xi_{k\nu}$ geordnet werden, die Glieder $l_{j\nu}^{\text{ter}}$ Dimension die niedrigsten, die überhaupt vorkommen; oder auch — nach der in Kap. V. § 6 angeführten Ausdrucksweise —

*) Dieser Satz wurde für den in der Literatur bisher allein behandelten Fall $k = 2$, der die Theorie der algebraischen Kurven, resp. der algebraischen Funktionen einer Veränderlichen umfaßt, von M. Noether zuerst ausgesprochen. („Zur Theorie des eindeutigen Entsprechens algebraischer Gebilde von beliebig vielen Dimensionen“. Math. Annalen Bd. II. 1870. pag. 314. In strengerer Ausführung: „Über einen Satz aus der Theorie der algebraischen Funktionen“. Math. Annalen Bd. VI. 1873. pag. 351.) Über die weitere Literatur des Satzes vergleiche man den „Bericht über die Entwicklung der Theorie der algebraischen Functionen“ von Brill und Noether im III. Bande der „Jahres-Berichte der deutschen Mathematiker-Vereinigung“ 1894. pag. 347.

$\xi_{1\nu}, \ldots, \xi_{k\nu}$ ein $l_{j\nu}$-faches Element der Mannigfaltigkeit $\lambda_{jj} = 0$. Wie schon früher, sei $c_{i\nu}$ die analog definierte Zahl für R_i. Die notwendige und hinreichende Bedingung dafür, daß Φ das Divisorensystem $(F_1, \ldots, F_k)$ enthalte, läßt sich dann folgendermaßen aussprechen:

Es müssen sich Formen $H_{1\nu}, \ldots, H_{k\nu}$ von der Beschaffenheit bestimmen lassen, daß in der Entwicklung von

$$\Phi - \sum_{i=1}^{k} H_{i\nu} F_i$$

nach den Potenzprodukten der $x_1 - \xi_{1\nu}, \ldots, x_k - \xi_{k\nu}$ keine Glieder d_ν^{ter} oder niedrigerer Dimension vorkommen. Dabei genügt es jedenfalls $d_\nu = \sum_{j=1}^{k} (c_{j\nu} - l_{j\nu}) - k$ anzunehmen.

Nach den vorausgeschickten Entwicklungen ist der Beweis des Satzes sehr einfach; bevor wir auf ihn eingehn, möge aber noch die (auch auf den Satz des vorhergehenden Paragraphen bezügliche) Bemerkung eingeschaltet werden, daß die so ausgesprochene notwendige und hinreichende Bedingung für $\Phi \equiv 0 \pmod{F_1, \ldots, F_k}$ geradeso wie die frühere (§ 11) eine rationale ist; d. h. die Anwendung der vier Species und die Bestimmung des größten gemeinschaftlichen Teilers gegebener orthoider Formen entscheidet in einer endlichen Anzahl von Schritten darüber, ob jene Bedingungen sich erfüllen lassen.

Der Natur des Satzes nach sind jene Glieder von $H_{i\nu}$, deren Dimension die d_ν^{te} übersteigt, für die vorliegende Frage irrelevant; es genügt also die $H_{i\nu}$ als allgemeine Formen d_ν^{ter} Dimension anzunehmen, deren Koeffizienten einem bestimmten Gattungsbereiche angehören.

Jene Bedingung setzt sich demnach in ein System von linearen diophantischen Gleichungen für die Koeffizienten der H um, auf das wir nicht näher eingehn. Um so weniger, da ja für die praktische Entscheidung darüber, ob eine Darstellung

$\Phi = \sum_{i=1}^{k} H_i F_i$ existiert, und für die Bestimmung der H_i der Satz des § 11 uns viel einfachere Mittel an die Hand gibt.

Die Bedeutung des Noetherschen Satzes liegt vorwiegend in den durch ihn statuierten Eigenschaften der das Divisorensystem enthaltenden Formen Φ. Insbesondere möge sogleich betont werden, daß die jetzt gegebenen notwendigen und hinreichenden Bedingungen von einer auf die $x_1, \ldots, x_k$ ausgeübten (homogenen) linearen Transformation, wie unmittelbar ersichtlich, unabhängig sind.

Wenn wir nun endlich auf den Beweis des Satzes übergehn, ist wieder die Notwendigkeit der Bedingung evident, weil ja solche Formen H_i existieren, für welche $\Phi - \sum_{i=1}^{k} H_i F_i$ identisch Null wird.

Um die Bedingungen als hinreichende zu erweisen, bemerke man zuerst, des einfacheren Ausdrucks wegen, daß

$$\Psi \equiv 0 \pmod{\{a+1\}},$$

wenn $\{a+1\}$ als kurzes Symbol für das Divisorensystem

$$(\cdots, (x_1 - \xi_{1\nu})^{g_1} (x_2 - \xi_{2\nu})^{g_2} \cdots (x_k - \xi_{k\nu})^{g_k}, \cdots),$$
$$(g_1 + g_2 + \cdots + g_k = a + 1)$$

gebraucht wird, die Tatsache ausdrückt, daß die Form Ψ bei Entwicklung nach den Potenzprodukten der $x_1 - \xi_{1\nu}, x_2 - \xi_{2\nu}, \cdots$ keine Glieder der a^{ten} oder niedrigerer Dimension enthält.

Ist nun der ausgesprochenen Bedingung gemäß ein Formensystem $H_{i\nu}$ von der Beschaffenheit vorhanden, daß

$$\Phi - \sum_{i=1}^{k} H_{i\nu} F_i \equiv 0 \pmod{\{d_\nu + 1\}},$$

so wird

$$\lambda_{11}\Phi - H_{1\nu}\lambda_{11} F_1 - \sum_{i=\nu}^{k} \lambda_{11} H_{i\nu} F_i \equiv 0 \pmod{\{d_\nu + l_{1\nu} + 1\}},$$

also, wenn man statt $\lambda_{11} F_1$ nun R_1 einführt, auch ein Formensystem $H'_{i\nu}$ existieren, für welches

$$\lambda_{11}\Phi - H'_{i\nu} R_1 - \sum_{i=\nu}^{k} H'_{i\nu} F_i \equiv 0 \pmod{\{d_\nu + l_{1\nu} + 1\}}$$

wird. Multipliziert man wieder mit λ_{22} und führt R_2 ein und so fort, so gelangt man endlich zu einer Kongruenz

$$\Lambda\Phi - \sum_{i=1}^{k} K_{\nu i} R_i \equiv 0 \pmod{\{d_\nu + \sum_{j=1}^{k} l_{j\nu} + 1\}}.$$

Ist aber $d_\nu \geqq \sum_{j=1}^{k} (c_{j\nu} - l_{j\nu}) - k$, so wird

$$d_\nu + \sum_{j=1}^{k} l_{j\nu} + 1 \geqq \sum_{j=1}^{k} c_{j\nu} - k + 1,$$

und damit ist die in § 12 entwickelte hinreichende Bedingung erfüllt, also der Satz bewiesen.

Es ist selbstverständlich durchaus nicht ausgeschlossen, (und sogar mit Ausnahme der einfachsten „allgemeinen" Annahmen in der Tat der Fall), daß der Wert der Zahl d_ν, den wir unter allen Umständen wählen können, nämlich

$$\sum_{j=1}^{k} (c_{j\nu} - l_{j\nu}) - k,$$

größer als notwendig ist.

Es kann der Fall eintreten, daß an Stelle der gegebenen Bedingung schon

$$\Phi - \sum_{i=1}^{k} H_{i\nu} F_i \equiv 0 \pmod{\{d_\nu\}}$$

genügt. In diesem Falle muß aber für jedes Potenzprodukt d_ν^{ter} Dimension auch

$$(x_1 - \xi_{1\nu})^{h_1} \cdots (x_k - \xi_{k\nu})^{h_k} \equiv 0 \pmod{\{d_\nu + 1\}},$$
$$(h_1 + \cdots + h_k = d_\nu)$$

sein, und dies genügt auch. Ob nun diese Kongruenzbedingung erfüllt ist, wird durch die Möglichkeit der Auflösung einer Reihe von diophantischen Gleichungen, also in einer endlichen Anzahl von Schritten entschieden. Es ist demnach entweder d_ν die kleinste Zahl, die in den Noetherschen Bedingungen eintritt, oder man kann dafür $d_\nu - 1$ nehmen. Bei Fortsetzung dieses Verfahrens gelangt man daher durch eine Reihe von algebraischen Operationen zu einer kleinsten Zahl

e_ν, so daß zur Entscheidung, ob $\Phi \equiv 0 \pmod{F_1, \ldots, F_k}$ ist, die Vergleichung von Φ mit einer Entwicklung von $\sum_{i=1}^{k} H_i F_i$ nach Potenzprodukten von $x_1 - \xi_{1\nu}, \cdots, x_k - \xi_{k\nu}$ bis zu den Gliedern e_ν^{ter} Dimension (diese inbegriffen) notwendig und hinreichend ist, während man für $e'_\nu < e_\nu$ nur mehr notwendige, aber nicht hinreichende Bedingungen erhält.

Die so definierte und auch algebraisch bestimmte Zahl e_ν soll weiterhin als Charakteristik des Wurzelsystems $\xi_{1\nu}, \ldots, \xi_{k\nu}$ bezeichnet werden. Es ist für die Anwendungen des verallgemeinerten Noetherschen Satzes von Wichtigkeit, diese Charakteristik der einzelnen Wurzelsysteme aus den allgemeinen Eigenschaften des Divisorensystems $(F_1, \ldots, F_k)$ genauer zu bestimmen.

Theorie der Charakteristiken der Wurzelsysteme für den „einfachen" Fall.

§ 14. Das Gleichungssystem $F_i = 0$, $(i = 1, \ldots, k)$, in dem wir abermals $x_1, \ldots, x_k$ als Unbekannte auffassen, sei wieder von der k^{ten} Stufe, und

$$\xi_{1\nu}, \xi_{2\nu}, \ldots, \xi_{k\nu}$$

eines seiner in endlicher Anzahl vorhandenen Wurzelsysteme Es beginne ferner die Entwicklung von F_i nach Potenzprodukten der $x_1 - \xi_{1\nu}$, $x_2 - \xi_{2\nu}, \cdots$ mit den Gliedern $a_{i\nu}^{\text{ter}}$ Dimension, deren Komplex mit φ_i bezeichnet werde, so daß

$$F_i = \varphi_i + \varphi_i^{(a_{i\nu}+1)} + \cdots$$

wird, eine Tatsache, die wir im Anschluß an die schon gebrauchten Bezeichnungen durch die Kongruenz

$$F_i \equiv 0 \pmod{\{a_{i\nu}\}}$$

bezeichnen, in der jetzt selbstverständlich $a_{i\nu} \geqq 1$ ist.

Wir untersuchen nun den s. g. einfachen Fall*), der

*) Diese Benennung stammt für den Fall $k = 2$ von Noether (a. a. O.). Ist (A) die Gesamtheit der komplexen Zahlen, so hat man es

durch die Voraussetzung charakterisiert wird, daß das Gleichungssystem $\varphi_i = 0$ nur die eine Lösung $x_j = \xi_{j\nu}$ besitzt. Selbstverständlich ist dann

$$r_\nu = \text{Res.} \begin{pmatrix} \varphi_1, \ldots, \varphi_k \\ z_1, \ldots, z_k \end{pmatrix} \neq 0,$$

wenn wir noch des kürzeren Ausdrucks wegen $z_j = x_j - \xi_{j\nu}$ setzen.

Setzt man noch

$$A_\nu = a_{1\nu} a_{2\nu} \ldots a_{k\nu},$$

so hat man unter dieser Voraussetzung

$$r_\nu z_j^{A_\nu} = \mu_{j1}\varphi_1 + \cdots + \mu_{jk}\varphi_k, \tag{1}$$

wo μ_{ji} eine homogene Form $(A_\nu - a_{j\nu})^{\text{ter}}$ Dimension von $z_1, \ldots, z_k$ ist.

Bildet man nun nach Anweisung des § 10 die Formenreihe $R_1, \ldots, R_k$ in Bezug auf $\varphi_1, \ldots, \varphi_k$, so haben auch die Gleichungen $R_1 = 0, \varphi_2 = 0, \ldots, \varphi_k = 0$ nur das eine Wurzelsystem $z_1 = 0, \ldots, z_k = 0$ und so fort. Man hat es also immer wieder mit dem einfachen Falle, andrerseits auch immer mit homogenen Formen zu tun. Es werden daher die dem zu Beginn des § 13 ausgesprochenen Satze gemäß bestimmten Zahlen $c_{j\nu}$ und $l_{j\nu}$ die Eigenschaft besitzen, daß $c_{j\nu} - l_{j\nu} = a_{j\nu}$ ist, und daraus folgt unmittelbar, daß die Charakteristik des Wurzelsystems $z_j = 0$ in Bezug auf das Gleichungssystem $\varphi_i = 0$ nicht größer als $\sum_{i=1}^{k} a_{i\nu} - k$ ist.

§ 15. Daß dasselbe auch für das Gleichungssystem $F_i = 0$ stattfindet, soll nun nachgewiesen werden.

Wir zeigen zu diesem Zwecke zuerst, daß man Formen $M_i (i = 1, \ldots, k)$, deren Entwicklung nach den Potenz-

---

mit der „Geometrie im Raume von k Dimensionen" zu tun, und der „einfache Fall" ist in geometrischer Ausdrucksweise derjenige, wo der Punkt $(\xi_{1\nu}, \ldots, \xi_{k\nu})$ wohl auf allen $k-1$-fachen Mannigfaltigkeiten $F_i = 0$ liegt, es aber keine „gerade Linie" gibt, die in diesem Punkte sämtliche Mannigfaltigkeiten $F_i = 0$ zugleich $(a_{i\nu} + 1)$-punktig berührt.

produkten der z genau mit den Gliedern $(A_\nu - a_{i\nu})^{\text{ter}}$ Dimension beginnt, ferner noch so wählen kann, daß in der Entwicklung von

$$z_1^{A_\nu} - \sum_{i=1}^{k} M_i F_i$$

nach den Potenzprodukten der z alle Glieder, deren Dimension kleiner als eine genügend groß gewählte Zahl g ist, wegfallen.

Dementsprechend setzen wir

$$M_i = M_{i0} + M_{i1} + M_{i2} + \cdots$$

und, wie früher,

$$F_i = \varphi_i + \varphi_i^{(a_{i\nu}+1)} + \varphi_i^{(a_{i\nu}+2)} + \cdots .$$

Die Entwicklung von M_i ist so zu verstehn, daß M_{ih} eine homogene Form der z von der Dimension $A_\nu - a_{i\nu} + h$ ist.

Dann muß zuerst

$$\sum_{i=1}^{k} M_{i0}\varphi_i = z_1^{A_\nu}$$

sein, und dies wird nach (1) erreicht, wenn man

$$M_{i0} = \frac{1}{r_\nu}\mu_{1i}$$

setzt. Es sind jetzt die Formen M_{i1} so zu bestimmen, daß

$$\sum_{i=1}^{k} M_{i1}\varphi_i = -\sum_{i=1}^{k} M_{i0}\varphi_i^{(a_{i\nu}+1)}$$

wird. Rechts steht eine homogene Form der z von der Dimension $A_\nu + 1$; nun ist aber schon

$$A_\nu = a_{1\nu} \cdots a_{k\nu} > \sum_{i=1}^{k} (a_{i\nu} - 1),$$

also kann man jedenfalls, nach den für das Gleichungssystem $\varphi_i = 0$ bewiesenen Sätzen:

$$-\sum_{i=1}^{k} M_{i0}\varphi_i^{(a_{i\nu}+1)} = \sum_{i=1}^{k} \mu_{i1}\varphi_i$$

erhalten und dementsprechend

$$M_{i1} = -\mu_{i1}$$

wählen. Wenn man in der angegebenen einfachen Weise fortfährt und

$$M_i = M_{i0} + M_{i1} + \cdots + M_{i,g-a_{iv}}$$

setzt, so werden die so erhaltenen Formen in der Tat den ausgesprochenen Bedingungen genügen. Wählt man endlich $g > A_v + e_v$, so wird jedes Glied in der Entwicklung von $z_1^{A_v} - \sum_{i=1}^{k} M_i F_i$ als Produkt zweier Faktoren darstellbar seien, deren jeder ein Potenzprodukt der z ist, und zwar der eine (P') von der Dimension A_v, der andere (P'') von höherer als e_v^{ter} Dimension, wo e_v die Charakteristik des Wurzelsystems $z_j = 0$ in Bezug auf $F_i = 0$ bedeutet. Dementsprechend schreiben wir

$$z_1^{A_v} - \sum_{i=1}^{k} M_i F_i = \sum_{h=1}^{H} P_h' P_h''.$$

Multipliziert man jedes Glied mit der nach § 10 definierten Form

$$\frac{R_1(x_1)}{(x_1 - \xi_{1\nu})^{c_{1\nu}}} = (x_1 - \xi_{11})^{c_{11}} \cdots,$$

so erhält man, wenn wieder $z_j = x_j - \xi_{j\nu}$ gesetzt wird,

$$\overline{R}_1(x_1) = \sum_{i=1}^{k} \overline{M}_i F_i + \sum_{h=1}^{H} P_h' (P_h''(x_1 - \xi_{11})^{c_{11}} \cdots).$$

Da nun bei einer passend gewählten linearen Transformation zwei verschiedene Wurzelsysteme auch aus durchweg verschiedenen Größen bestehn, gibt die Entwicklung des hinzugefügten Faktors nach den Potenzprodukten von $x_1 - \xi_{1\nu}, \ldots, x_k - \xi_{k\nu}$ ein nicht verschwindendes Glied von der Dimension Null, und es beginnt daher die Entwicklung von $\overline{R}_1(x_1), \overline{M}_1, \ldots, \overline{M}_k$, nach diesen Potenzprodukten mit den Gliedern derselben Dimension, wie die von $z_1^{A_v}$ und $M_1, \ldots, M_k$.

Man sieht ferner, daß die Formen

$$P_k''(x_1 - \xi_{11})^{c_{11}} \ldots$$

den Bedingungen des Noetherschen Satzes genügen. Für das Wurzelsystem $\xi_{1\nu}, \ldots, \xi_{k\nu}$ ist dies einfach die Folge des Umstandes, daß P_h'', nach den Potenzprodukten von $x_1 - \xi_{1\nu}, \cdots, x_k - \xi_{k\nu}$ entwickelt, nur Glieder von höherer als der e_ν^{ten} Dimension ergibt. Für die übrigen Wurzelsysteme erhellt dasselbe aus der Tatsache, daß die betrachtete Form durch $(x_1 - \xi_{11})^{c_{11}}$ u. s. w. teilbar ist, also die Kongruenzen (K_ν) des § 12 erfüllt sind.

Man hat demnach

$$\sum_{h=1}^{H} P_h'(P_h''(x_1 - \xi_{11})^{c_{11}} \ldots) = \sum_{i=1}^{k} \bar{N}_i F_i,$$

und die Formen $\bar{N}_i$ beginnen — wegen der entsprechenden Eigenschaft der P_h' — bei der Entwicklung nach den Potenzprodukten von $x_1 - \xi_{1\nu}, \ldots, x_k - \xi_{k\nu}$ mit Gliedern, deren Dimension nicht kleiner als A_ν sein kann.

Setzt man nun

$$\bar{M}_i + \bar{N}_i = \bar{\lambda}_{1i},$$

so erhält man

$$\bar{R}_1(x_1) = \sum_{i=1}^{k} \bar{\lambda}_{1i} F_i,$$

wo die Entwicklung von $\bar{R}_1(x_1)$ nach jenen Potenzprodukten genau mit den Gliedern A_ν^{ter} Dimension, die von $\bar{\lambda}_{1i}$ mit den Gliedern von zumindest $(A_\nu - a_{i\nu})^{\text{ter}}$ Dimension beginnt.

Man kann mit dem Formensysteme $\bar{R}_1(x_1), F_2, \ldots, F_m$ genau ebenso verfahren, da wir es nach den Erörterungen in § 10 immer wieder mit dem „einfachen" Falle zu tun haben. So entsteht die Formenreihe

$$\bar{R}_\mu(x_\mu) = \sum_{\varrho=1}^{\mu-1} \bar{\lambda}_{\mu\varrho} \bar{R}_\varrho + \sum_{j=\mu}^{k} \lambda_{\mu j} F_i \qquad (\bar{R}_\mu)$$
$$(\mu = 1, \ldots, k),$$

die in dem Satze des § 13 benutzt werden kann. Nun ist

aber die dort auftretende Zahl $c_{jv} - l_{jv} \leqq a_{jv}$, und es ergibt sich somit der folgende Satz:

Die Charakteristik des Wurzelsystems $\xi_{1v}, \ldots, \xi_{kv}$ für das Gleichungssystem $F_1 = 0, \ldots, F_k = 0$ ist im einfachen Falle nicht größer als $\Sigma a_{iv} - k$, wenn $\xi_{1v}, \ldots, \xi_{kv}$ ein a_{iv}-faches Element der Mannigfaltigkeit $F_i = 0$ ist.

Der Hilbertsche Satz.

§ 16. Sind wieder $F_i(x_1, \ldots, x_m)$, $(i = 1, \ldots, k)$ dem orthoiden Bereiche (A) entstammende Formen, jetzt aber

$$(F_1, F_2, \ldots, F_k)$$

ein ganz beliebiges Divisorensystem, so erkennt man unmittelbar, daß, wenn für irgend eine Form Φ

$$\Phi \equiv 0 \pmod{F_1, F_2, \ldots, F_k}$$

sein soll, wegen $\Phi = \sum_{i=1}^{k} H_i F_i$ die Gleichung $\Phi = 0$ für jedes Wurzelsystem des Gleichungssystems $F_i = 0$ befriedigt sein muß. Aber schon der Fall der der Hauptklasse angehörigen Divisorensysteme zeigt, daß diese notwendige Bedingung durchaus nicht hinreichend ist. Es gilt jedoch in diesem Falle der folgende in voller Allgemeinheit von D. Hilbert*) aufgestellte Satz:

Es seien

$$G_1, G_2, \ldots, G_l$$

irgend welche Formen, die für jedes Wurzelsystem, das dem Gleichungssysteme $F_i = 0$ genügt, verschwinden. Dann gibt es eine positive ganze Zahl r, die durch das Divisorensystem $(F_1, \ldots, F_k)$ vollständig bestimmt ist, von der Beschaffenheit, daß

*) „Über die vollen Invariantensysteme". Math. Annalen, Bd. XLII. 1893. pag. 320.

$$G_{j_1} G_{j_2} \ldots G_{j_r} \equiv 0 \pmod{F_1, \ldots, F_k}$$

wird, wenn $G_{j_1}, \ldots, G_{j_r}$ irgend welche Formen aus der Reihe $G_1, \ldots, G_l$ bedeuten.

Statt dem ziemlich komplizierten Beweisgange Hilberts zu folgen, zeigen wir, daß der Satz ein einfaches Corollar der in Kap. V entwickelten allgemeinen Eliminationstheorie ist.

Wir bemerken vor allem, daß die im Hilbertschen Satze ausgedrückte Tatsache von irgend einer auf die Formen F und G zugleich ausgeübten (homogenen) linearen Transformation völlig unabhängig ist. Diese Bemerkung kann für den Beweis verwertet werden, indem wir voraussetzen, daß jene lineare Transformation, die der Bildung der Gesamtresolvente des Gleichungssystems $F_i = 0$ vorausgeht, auch schon die Formen G zu regulären transformiert*). Es sei $\Phi_t = 0$ die Gesamtresolvente des Gleichungssystems $F_i = 0$ (Kap. V. § 4) und P_{hj_h} irgend ein irreduzibler Teiler von Φ_t. Der Annahme nach verschwindet dann G_j für jedes Wertsystem, das den Gleichungen

$$P_{hj_h}\left(\sum_{i=1}^{m} t_i x_i, x_{h+1}, \ldots, x_{m-1}\right) = 0$$

genügt, wo die t_i als Unbestimmte zu fassen sind. Setzt man nun $x = \Sigma x_i t_i$ an Stelle von x_m, so geht G_j, mit einer entsprechenden Potenz von t_m multipliziert, in $\overline{G}_j$ über, und es muß $\overline{G}_j$ durch $P_{hj_h}(x, x_{h+1}, \ldots, x_{m-1})$ teilbar sein. Sonst ergäbe das gewöhnliche Divisionsverfahren einen Ausdruck

$$R = \overline{G}_j - P_{hj_h} Q,$$

der in x von niedrigerem Grade als P_{hj_h} ist und nicht verschwindet. Wählt man aber die Werte $x_{h+1} = \xi_{h+1}, \ldots, x_{m-1} = \xi_{m-1}$ so, daß die Discriminante von P_{hj_h} nach x nicht Null ist, so müßte es einen entsprechenden Wert

*) Der Ausnahmefall, in dem ein G keine der Unbestimmten $x_1, \ldots, x_m$ enthält, braucht nicht berücksichtigt zu werden.

$$x = \sum_{i=1}^{h} t_i \xi_i' + \sum_{j=h+1}^{m-1} t_j \xi_j + t_m \xi_m'$$

geben, für welchen P_{hj_h} gleich Null wird, während R nicht verschwindet. Für diesen Wert wäre auch $\overline{G}_j$ nicht Null, d. h. G_j würde im Gegensatze zur Annahme nicht für alle durch das Gleichungssystem $P_{hj_h} = 0$ gegebene Werte verschwinden. — Ebenso muß $\overline{G}_j$ durch jeden andern irreduzibeln Teiler von Φ_t teilbar sein.

Ist demnach r der größte Exponent, mit welchem irgend ein irreduzibler Teiler in Φ_t vorkommt, so ist

$$\overline{G}_{j_1} \overline{G}_{j_2} \dots \overline{G}_{j_r}$$

durch Φ_t teilbar, also wie diese Form selbst,

$$\overline{G}_{j_1} \overline{G}_{j_2} \cdots \overline{G}_{j_r} \equiv 0 \left(\text{mod. } F_1, \cdots, F_k, x - \sum_{i=1}^{m} t_i x_i\right).$$

Setzt man demnach $x = \sum_{i=1}^{m} t_i x_i$ und vergleicht die Koeffizienten der beiderseits stehenden Potenzprodukte der t, so erhält man in der Tat

$$G_{j_1} G_{j_2} \dots G_{j_r} \equiv 0 \text{ (mod. } F_1, \dots, F_k),$$

was zu beweisen war.

Achtes Kapitel.

Arithmetische Theorie der linearen diophantischen Probleme.

Die absoluten Primsysteme in $[[1], x_1, x_2, \ldots, x_k]$.

§ 1. Es seien $S_1, S_2, \ldots$ irgend welche rationale und ganze Formen der Unbestimmten $x_1, x_2, \ldots, x_k$. Das aus ihnen gebildete Divisorensystem $(S_1, S_2, \ldots)$ soll in der Folge kurz durch das Symbol (S) bezeichnet werden. Es kann sodann eine endliche Reihe von Formen

$$C_0, C_1, \ldots, C_{s-1}$$

des Bereichs $[[1], x_1, \ldots, x_k]$ von der Beschaffenheit existieren, daß jede Form des angegebenen Bereichs mit einer und nur einer der Formen C kongruent mod. (S) ist. Diese Eigenschaft soll weiterhin durch den Ausdruck bezeichnet werden, daß „für das Divisorensystem (S) ein vollständiges Restsystem $C_0, C_1, \ldots, C_{s-1}$ existiert". Dabei kann selbstverständlich irgend ein C_i durch jede andere mod. (S) mit C_i kongruente Form C_i' ersetzt werden.

Ist ferner ein dem Divisorensysteme (S) entsprechendes vollständiges Restsystem bekannt, und auch ein Verfahren gegeben, um die mit einer beliebigen Form F kongruente Form C_i des Restsystems zu bestimmen, so kann die „Auflösung der linearen Kongruenz"

$$AX \equiv B \pmod{(S)}$$

als erledigt betrachtet werden; dabei sollen zwei mod. (S)

kongruente Lösungen als nicht verschieden angenommen werden. Denn da nur die Wurzeln $C_0, C_1, \ldots, C_{s-1}$ existieren können, genügt es, durch eine endliche Reihe von Versuchen festzustellen, welche der Größen $AC_0, AC_1, \ldots$ mit der Größe B (die selbst $\equiv C_j$) kongruent sind.

Ist insbesondere das vorgelegte Divisorensystem ein absolutes Primsystem — ein solches soll von nun an kurz mit (P) bezeichnet werden — und A nicht $\equiv 0 \pmod{(P)}$, so hat die Kongruenz

$$AX \equiv B \pmod{(P)}$$

eine und nur eine Wurzel.

Es muß nämlich $(A, (P)) \simeq 1$ sein, da dieses Divisorensystem in (P) enthalten und doch nicht $\simeq (P)$ sein kann, da in dem letzteren Falle im Gegensatze zur Annahme $A \equiv 0 \pmod{(P)}$ sein müßte. Diese Äquivalenz besagt aber, daß eine Identität von der Gestalt

$$\lambda A + \mu_0 P_0 + \mu_1 P_1 + \cdots = 1$$

bestehn muß, oder also eine Form λ existiert, für die

$$\lambda A \equiv 1 \pmod{(P)},$$

also auch

$$X \equiv \lambda B \pmod{(P)}$$

ist; da diese Größe der Kongruenz in der Tat genügt, ist sie ihre einzige Wurzel.

Unter den früher festgesetzten Annahmen bestimmt sich diese Wurzel wieder in einer endlichen Versuchsreihe.

Genügt nun wieder das Divisorensystem (S) den oben gemachten Annahmen, so ergibt sich für die rationalen und ganzen Formen der Unbestimmten $x_1, \ldots, x_k, x_{k+1}, \ldots, x_m$ eine elementare Theorie der „Teilbarkeit mod. (S)".

„Eine Form F ist mod. (S) durch die Form G teilbar", wenn es eine dritte Form H von der Beschaffenheit gibt, so daß:

$$F \equiv GH \pmod{(S)}.$$

Da (S) die Unbestimmten $x_{k+1}, \ldots, x_m$ nicht enthält, kann

$F - GH \equiv 0 \pmod{(S)}$ nur dann stattfinden, wenn jeder Koeffizient der verschiedenen Potenzprodukte von $x_{k+1}, \ldots, x_m$ schon für sich $\equiv 0 \pmod{(S)}$ ist, und daraus folgt, daß G und H, wenn man die Glieder, deren Koeffizienten $\equiv 0 \pmod{(S)}$ sind, wegläßt (was ja hier keine Änderung statuiert, da die Formen F, G, H immer $\pmod{(S)}$ zu verstehn sind), in $x_{k+1}, \ldots, x_m$ nicht vom höheren Grade sein kann als F. Da endlich die Koeffizienten der verschiedenen Potenzprodukte von $x_{k+1}, \ldots, x_m$ nur die in dem vollständigen Restsysteme auftretenden Formen sein können, so sieht man, daß F nur eine endliche Anzahl von Teilern haben kann, die durch eine endliche Versuchsreihe bestimmt werden, und zwar ergibt diese mit G auch den „komplementären" Teiler H.

In völliger Analogie mit der gewöhnlichen Teilbarkeitstheorie der rationalen und ganzen Formen heißen die Formen F und G „äquivalent $\pmod{(S)}$", wenn F und G dieselben Teiler $\pmod{(S)}$ besitzen oder also auch, wenn zu gleicher Zeit F durch G und G durch F teilbar $\pmod{(S)}$ ist.

Es heiße endlich wieder F „irreduzibel $\pmod{(S)}$", wenn jeder Teiler von F mit der Einheit oder mit F selbst $\pmod{(S)}$ äquivalent ist.

Wir betrachten nun das spezielle Divisorensystem

$$(M^{(k)}) = (M_k, \ldots, M_2, M_1, n_0),$$

wo n_0 eine von 1 verschiedene rationale und ganze positive Zahl bedeute und allgemein

$$M_i = x_i^{n_i} + \varphi_{i1} x_i^{n_i - 1} + \cdots + \varphi_{in_i}$$

ist, wo $\varphi_{i1}, \ldots, \varphi_{in_i}$ wieder rationale und ganze Formen der Unbestimmten $x_1, \ldots, x_k$ mit Ausschluß von $x_i, x_{i+1}, \ldots, x_k$ bedeuten; es sind also insbesondere $\varphi_{11}, \ldots, \varphi_{1n_1}$ rationale und ganze Zahlen.

Wendet man auf eine beliebige Form $F(x_1, x_2, \ldots, x_k)$ das gewöhnliche Divisionsverfahren an, so erhält man

$$F = M_k Q_k + R_k,$$
$$R_k = M_{k-1} Q_{k-1} + R_{k-1},$$
$$\cdots\cdots\cdots\cdots$$
$$R_2 = M_1 Q_1 + R_1;$$

setzt man weiter in R_1 für die Zahlenkoeffizienten die kleinsten nicht negativen Reste mod. n_0, oder also

$$R_1 = n_0 Q_0 + R_0,$$

so wird schließlich:

$$F \equiv R_0 \ (\text{mod. } M_k, \ldots, M_1, n_0).$$

Seiner Bildung nach kann aber R_0 in x_i den Grad $n_i - 1$ nicht übersteigen, während als Koeffizienten der einzelnen Potenzprodukte von $x_1, \ldots, x_k$ in R_0 nur die Zahlen $0, 1, \ldots, n_0 - 1$ auftreten können.

Die so erhaltenen Formen, deren Anzahl augenscheinlich $n_0^{n_1 n_2 \cdots n_k}$ ist, sind aber auch alle mod. $(M^{(k)})$ voneinander verschieden; denn, bezeichnet man sie mit

$$\varrho_0, \varrho_1, \ldots,$$

so müßte, da auch $\varrho_r - \varrho_s$ in x_i den Grad n_i nicht erreicht, und die Zahlenkoeffizienten, vom Vorzeichen abgesehn, $n_0 - 1$ nicht überschreiten, aus

$$\varrho_r - \varrho_s = G_k M_k + G_{k-1} M_{k-1} + \cdots + G_1 M_1 + G_0 n_0$$

nach jenem Divisionsverfahren eine ebensolche Darstellung von $\varrho_r - \varrho_s$ folgen, wo der Reihe nach $G_k = 0, \ldots, G_1 = 0$ ist, und dann $\varrho_r - \varrho_s$ durch n_0 teilbar sein muß; also wird endlich wegen der für die Zahlenkoeffizienten statuierten Bedingung identisch $\varrho_r = \varrho_s$.

Für das Divisorensystem $M^{(k)}$ ist demnach $\varrho_0, \varrho_1, \ldots$ ein vollständiges Restsystem, und alle Darlegungen dieses Paragraphen sind darauf anwendbar.

§ 2. Die soeben definierten Divisorensysteme $M^{(k)}$ sollen nun weiter spezialisiert werden; und zwar sei dieses speziellere System

$$(P^{(k)}) = (P_k, P_{k-1}, \ldots, P_1, p_0),$$

wo p_0 eine natürliche Primzahl und P_i eine rationale und ganze Form sei, die alle für M_i statuierten Eigenschaften besitze, weiter aber noch mod. $(P^{(i-1)})$, d. h. mod. $(P_{i-1}, \ldots, P_1, p_0)$ irreduzibel sein soll. Die so definierten Systeme, die kurz als „P-Systeme“ k — 1ter Stufe*) bezeichnet werden mögen, gewinnen durch die folgenden beiden Sätze eine grundlegende Bedeutung für die arithmetische Theorie der algebraischen Größen:

I. Jedes System $(P^{(k)})$ ist ein absolutes Primsystem im Bereiche der rationalen und ganzen Formen, die keine andern Unbestimmten als die in $P_k, \ldots, P_1, p_0$ vorkommenden enthalten, und ein Primsystem schlechtweg im Bereiche jener rationalen und ganzen Formen, die außer diesen noch weitere Unbestimmte $x_{k+1}, \ldots, x_m$ enthalten.

II. Jedes absolute Primsystem im Bereiche der rationalen und ganzen Formen von $x_1, \ldots, x_k$ ist einem

*) Die P-Systeme bilden das naturgemäße Analogon für den Primzahl-Begriff im Bereiche der rationalen und ganzen Formen und sind für eine Behandlung der arithmetischen Probleme in diesen Bereichen unerläßlich. Sie sind bisher nur für den Fall $m = 1$ betrachtet worden, zuerst von Schönemann (Journal f. r. u. a. Math., Bd. 31 u. 32. 1846); dieser einfachste Fall findet sich aber auch schon, wie sich später herausgestellt hat, in Gauß' Nachlaß (Werke, Bd. II. pag. 197).

Der ganze Inhalt dieses Kapitels ist demgemäß neu und ergänzt eine wesentliche Lücke in der arithmetischen Theorie der algebraischen Größe. Wir sind erst durch die hier entwickelten Resultate in den Stand gesetzt, die zwei großen Probleme der allgemeinen Arithmetik — wirkliche Aufstellung der Fundamentalsysteme und wirkliche Zerlegung einer ganzen Größe in ihre irreduzibeln Teiler — in Kap. IX vollständig zu lösen.

Dabei treten aber noch der in Kap. III gegebene Begriff der Resolventenform und die auf diesen gegründete Verallgemeinerung der Kroneckerschen Eliminationsmethode als neue methodische Hilfsmittel von fundamentaler Bedeutung hinzu.

Diese kurzen Bemerkungen mögen auf die naturgemäße Notwendigkeit und Folgerichtigkeit jenes Systems einer Theorie der algebraischen Größen hinweisen, das der Verfasser in diesem Buche durchzuführen versucht hat.

Systeme $(P^{(k)})$ äquivalent, so daß diese Systeme die Gesamtheit der absoluten Primsysteme in einer bestimmten „kanonischen" Gestalt darstellen.

Der zweite Satz wird vorläufig nur erwähnt, um die Bedeutung der P-Systeme schon hier klarzustellen; sein Beweis, der in § 8 enthalten ist, erfordert tiefer liegende Hilfsmittel. Jetzt beschäftigen wir uns mit den Vorbereitungen zum Beweise des ersten Satzes.

Mit dem Systeme $(P^{(k)})$ sind auch die Systeme

$$\begin{aligned}(P^{(0)}) &= (p_0)\\ (P^{(1)}) &= (P_1, p_0)\\ &\cdots\cdots\cdots\\ (P^{(k-1)}) &= (P_{k-1}, \ldots, P_1, p_0)\end{aligned}$$

gegeben, von denen jedes das folgende, und endlich $(P^{(k-1)})$ auch $(P^{(k)})$ enthält.

Für $k = 0$ ist das Divisorensystem $(P^{(0)})$ nichts anderes als die Primzahl p_0, der Satz also in diesem einfachsten Falle jedenfalls richtig. Allgemein wird er durch vollständige Induktion erschlossen, indem wir annehmen, daß der Satz für $(P^{(0)}), \ldots, (P^{(k)})$ gilt, und dann auf dieser Grundlage denselben Satz auch für $(P^{(k+1)})$ beweisen.

Dieser Beweis durch vollständige Induktion beruht wesentlich auf den Eigenschaften der rationalen und ganzen Formen, die sich bei ihrer Betrachtung mod. $(P^{(k)})$ darbieten, wo $(P^{(k)})$ schon als absolutes Primsystem in $[[1], x_1, \ldots, x_k]$ vorausgesetzt wird.

Was zuerst die rationalen und ganzen Formen von $x_1, \ldots, x_k$ betrifft, so besitzen sie für das Divisorensystem $(P^{(k)})$ ein vollständiges Restsystem; insbesondere geben die früher aufgestellten Formen

$$\varrho_0, \varrho_1, \cdots$$

ein solches, wo man noch $\varrho_0 = 0$, $\varrho_1 = 1$ nehmen kann.

Diese Formen ϱ, wenn auch nur in endlicher Anzahl vorhanden, bilden einen „Bereich", in welchem die Addition und die Multiplikation in folgender Weise definiert werden kann. Die Summe, resp. das Produkt von ϱ_r und ϱ_s sei jene Form

des Restsystems, die mit den nach den gewöhnlichen Regeln der Algebra gebildeten Formen $\varrho_r + \varrho_s$, resp. $\varrho_r \varrho_s$ kongruent mod. $(P^{(k)})$ ist

Wenn wir aber festsetzen, daß sämtliche Formen, die $\equiv \varrho_r$ mod. $(P^{(k)})$ sind, nur als verschiedene Zeichen derselben Form ϱ_r zu betrachten sind, so können wir auch sagen, daß die Addition und Multiplikation der Formen ϱ nach den gewöhnlichen Regeln der Algebra erfolgt; dabei soll nur, um diese Verknüpfung von der Addition und Multiplikation der Formen im gewöhnlichen Sinne zu unterscheiden, jetzt in den entsprechenden Aussagen ein von dem früheren verschiedenes Gleichheitszeichen benutzt werden. Als solches bietet sich unmittelbar das Zeichen $\equiv$ mod. $(P^{(k)})$. Damit hat die Aussage

$$F \equiv \varrho_r \left(\text{mod. } (P^{(k)})\right)$$

eine doppelte Bedeutung gewonnen, die wohl sehr einfach, beinahe selbstverständlich ist, aber trotzdem, weil sie für die Methodik der arithmetischen Untersuchungen von geradezu grundlegender Bedeutung ist, so ausführlich auseinandergesetzt werden mußte.

Das so als „Bereich" aufgefaßte vollständige Restsystem oder, wie wir jetzt auch sagen können, der Bereich

$$\text{„}[[1], x_1, \ldots, x_k] \left(\text{mod. } (P^{(k)})\right)\text{"}$$

besitzt demnach ein gewöhnliches Additions- und Multiplikationsgesetz, insbesondere muß, da $(P^{(k)})$ ein Primsystem ist, mit immer auch

$$AB \equiv 0 \left(\text{mod. } (P^{(k)})\right)$$

$$A \equiv 0 \quad \text{oder} \quad B \equiv 0 \left(\text{mod. } (P^{(k)})\right)$$

sein; und die Kongruenz $AX \equiv B$ mod. $(P^{(k)})$ hat, wenn A nicht $\equiv 0$, immer eine und nur eine Wurzel. Der Bereich enthält auch die absolute Einheit und besitzt demnach alle Eigenschaften eines orthoiden Bereichs, mit Ausnahme einer einzigen, da in der Reihe

$$1, 1+1, \cdots$$

die Null jetzt in der Tat vorkommt.

Um uns kurz ausdrücken zu können, wollen wir einen Bereich, in dem die Reihe

$$1, 1+1, \cdots$$

die Null enthält, der aber sonst alle Eigenschaften eines holoiden, resp. orthoiden Bereichs besitzt, als pseudoholoiden, resp. pseudoorthoiden Bereich bezeichnen.

Der Bereich $[[1], x_1, \ldots, x_k] \left(\text{mod. } (P^{(k)})\right)$ ist also ein pseudoorthoider Bereich.

Genau dieselben Betrachtungen zeigen, daß der Bereich $[[1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m] \left(\text{mod. } (P^{(k)})\right)$ ein pseudoholoider Bereich ist. Dabei hat man nur die Formen von $x_1, \ldots, x_m$ als Formen von $x_{k+1}, \ldots, x_m$ zu schreiben und die als Koeffizienten auftretenden Formen von $x_1, \ldots, x_k$ wieder mod. $(P^{(k)})$ aufzufassen; insbesondere folgt aus

$$FG \equiv 0 \left(\text{mod. } (P^{(k)})\right),$$

da auch in diesem Bereiche der Annahme nach $(P^{(k)})$ ein Primsystem ist,

$$F \equiv 0, \text{ oder } G \equiv 0 \left(\text{mod. } (P^{(k)})\right),$$

und dies ist wieder nur möglich, wenn sämtliche Koeffizienten von F oder von G (als Formen von $x_{k+1}, \ldots, x_m$ aufgefaßt) $\equiv 0 \left(\text{mod. } (P^{(k)})\right)$ sind. Der Bereich enthält also nur eine „Null". Endlich hat z. B. die Kongruenz

$$x_{k+1} X \equiv 1 \left(\text{mod. } (P^{(k)})\right)$$

keine Lösung, da ja sonst auch

$$0 \equiv 1 \left(\text{mod. } (P^{(k)})\right)$$

sein müßte.

Man erhält aus dem pseudoholoiden Bereiche

$$[[1], x_1, \ldots, x_m] \text{ mod. } (P^{(k)})$$

wieder den zugeordneten pseudoorthoiden Bereich $([1], x_1, \ldots, x_m)$ mod. $(P^{(k)})$ (siehe Kap. I. § 4), der aus sämtlichen Formenquotienten $\frac{F}{G}$ besteht, wo G von 0 $\left(\text{mod. } (P^{(k)})\right)$ verschieden ist.

Auf dieser Grundlage baut sich eine Theorie der Teilbarkeit der Formen des Bereichs $[[1], x_1, \ldots, x_m] \bmod. (P^{(k)})$ auf, die wir nicht ausführlich auseinanderzusetzen brauchen, da sie sich Wort für Wort mit den Auseinandersetzungen in Kap. III. § 1, 2, 4—17 deckt, wenn man nur statt des Zeichens „=" überall „$\equiv \pmod. (P^{(k)})$" setzt.

Jene Eigenschaft der holoiden, resp. orthoiden Bereiche, die nun fehlt, wird nämlich nur bei dem Satze benutzt, daß jede Form durch eine bestimmte Transformation, deren Determinante gleich Eins, und deren Koeffizienten rationale, resp. rationale und ganze Zahlen sind, regulär wird. Von diesem Satze wird aber, abgesehn von § 3, der ein unerhebliches Detail behandelt, nur in der Theorie der Resolventenform und den sich auf diese stützenden Erörterungen (§ 18 ff.) Gebrauch gemacht*).

Dabei tritt aber noch die weitere wesentliche Vereinfachung ein, daß der Bereich

$$[[1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m] \bmod. (P^{(k)}),$$

dessen Formen wir nun als Formen von $x_{k+1}, \ldots, x_m$ mit Koeffizienten aus $[[1], x_1, \ldots, x_k]$, mod. $(P^{(k)})$ auffassen, da dieser ein pseudoorthoider Bereich ist, ein vollständiger pseudoholoider Bereich ist. Dabei ist die Bezeichnung „vollständig" wieder wie früher so zu verstehn, daß zwei beliebige Formen des Bereichs immer einen „größten gemeinschaftlichen Teiler", allerdings jetzt mod. $(P^{(k)})$, besitzen, für dessen Darstellung wir in Kap. III. § 11 eine genaue Anweisung besitzen.

§ 3. Wir haben dann insbesondere nach § 15 und 16 des Kap. III die folgenden Sätze:

Sind

$$F = A_0 x^m + \cdots, \; G = B_0 x^n + \cdots$$

zwei Formen, deren Koeffizienten dem pseudoholoiden

*) Wie sich die Verhältnisse hier gestalten, wird später (§ 4) ausführlich auseinanderzusetzen sein.

Bereiche $[[1], x_1, \ldots, x_k, x_{k+1}, \ldots]$ mod. $(P^{(k)})$ angehören, ferner A_0 und B_0 nicht zugleich $\equiv 0$ mod. $P^{(k)}$), so ist

$$\text{Res.} \begin{pmatrix} F, & G \\ x, & 1 \end{pmatrix} \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

die notwendige und hinreichende Bedingung für die Existenz eines gemeinschaftlichen Teilers mod. $(P^{(k)})$ von F und G, der x wirklich enthält, d. h. mit keiner Größe des Bereichs $[[1], x_1, \ldots, x_k, x_{k+1}, \ldots]$ kongruent mod. $(P^{(k)})$ ist.

Es ist ferner auch jetzt:

$$\text{Res.} \begin{pmatrix} F, & G \\ x, & 1 \end{pmatrix} = G_1 F + F_1 G \ \left(\text{mod. } (P^{(k)})\right),$$

wo G_1 höchstens vom $n - 1^{\text{ten}}$, F_1 höchstens vom $m - 1^{\text{ten}}$ Grade in x ist.

Auf diesen Grundlagen fußend, ist der in § 2 angezeigte Beweis sehr einfach zu führen.

Es ist $(P^{(k)})$ ein absolutes Primsystem im Bereiche $[[1], x_1, \ldots, x_k]$; daß ebendasselbe für $(P^{(k+1)})$ im Bereiche $[[1], x_1, \ldots, x_k, x_{k+1}]$ stattfindet, kann ausführlicher so ausgesprochen werden, daß, wenn $F_1, F_2, \ldots$ irgend welche Formen dieses Bereichs sind, und $(P^{(k+1)})$ das Divisorensystem $(F_1, F_2, \ldots)$ enthält, ohne daß

$$(F_1, F_2, \ldots) \simeq (P^{(k+1)})$$

ist, die Äquivalenz $(F_1, F_2, \ldots) \simeq 1$ stattfinden muß.

Es kann in dem soeben angegebenen Falle $(F_1, F_2, \ldots)$ das Divisorensystem $(P^{(k+1)})$ nicht enthalten; denn in diesem Falle wäre ja, da auch das Umgekehrte stattfindet,

$$(F_1, F_2, \ldots) \simeq P^{(k+1)}.$$

Unter den Formen F gibt es also mindestens eine, z. B. F_1, die $(P^{(k+1)})$ nicht enthält, die also in andrer Ausdrucksweise nicht $\equiv 0$ mod. $(P^{(k+1)})$ ist. Es ist also

$$F_1 \equiv \varrho \ \left(\text{mod. } (P^{(k+1)})\right),$$

wo ϱ eine Form des für $P^{(k+1)}$ existierenden, früher angegebenen

vollständigen Restsystems und nicht Null ist. Demnach ist ϱ eine rationale und ganze Form von $x_1, \ldots, x_{k+1}$, die in x_i den Grad n_i nicht erreicht, und deren Koeffizienten Zahlen aus der Reihe $0, 1, \cdots, p_0 - 1$ sind, aber nicht sämtlich verschwinden.

Nun kann man jedenfalls eine Form λ so bestimmen, daß

$$\lambda\varrho \equiv 1 \ \left(\text{mod. } (P^{(k+1)})\right)$$

wird. Ist ϱ, was ja auch vorkommen kann, eine positive ganze Zahl, die dann kleiner als p_0 ist, so hat man zu diesem Zwecke eine von 0 verschiedene ganze Zahl zu wählen, die der Kongruenz

$$\lambda\varrho \equiv 1 \ (\text{mod. } p_0)$$

genügt. Ist hingegen ϱ eine wirkliche Form von $x_1, \ldots, x_{k+1}$, und z. B. x_i die letzte Unbestimmte dieser Reihe, die in ϱ wirklich vorkommt, so bemerke man, daß ϱ in x_i höchstens vom Grade $n_i - 1$ ist, während P_i eine mod. $(P^{(i-1)})$ irreduzible Form von der Gastalt $x_i^{n_i} + \cdots$ ist und die Unbestimmten $x_{i+1}, \ldots$ gleichfalls nicht enthält. Es kann also — alles mod. $(P^{(i-1)})$ verstanden — ϱ nicht durch P_i teilbar sein, und es können demnach ϱ und P_i überhaupt keinen gemeinschaftlichen Teiler besitzen, der x_i enthält. Es ist also, wenn man die Resultante von ϱ und P_i nach x_i mit σ_{i-1} bezeichnet:

$$\sigma_{i-1} \equiv \lambda_{i-1}\varrho + \mu_{i-1}P_i \ \left(\text{mod. } (P^{(i-1)})\right)$$

und mod. $(P^{(i-1)})$ von Null verschieden. Man kann nun jedenfalls nach den Voraussetzungen eine Form α bestimmen, für die

$$\alpha\sigma_{i-1} \equiv 1 \ \left(\text{mod. } (P^{(i-1)})\right)$$

wird. Mithin wird

$$\alpha\lambda_{i-1}\varrho \equiv 1 - \alpha\mu_{i-1}P_i \ \left(\text{mod. } (P^{(i-1)})\right)$$

oder, was dasselbe bedeutet, für $\lambda = \alpha\lambda_{i-1}$:

$$\lambda\varrho \equiv 1 \ \left(\text{mod. } (P^{(i)})\right),$$

und also auch

$$\lambda\varrho \equiv 1 \ \left(\text{mod. } (P^{(k+1)})\right).$$

Es ist aber

$$(F_1, P_{k+1}, \ldots, P_1, p_0) \simeq (\varrho, P_{k+1}, \ldots, P_1, p_0)$$

ein System, das mit $(P^{(k+1)})$ jedenfalls $(F_1, F_2, \ldots)$ enthält.

Dasselbe ist daher für

$$(\lambda\varrho, P_{k+1}, \ldots, P_1, p_0) \simeq (1, P_{k+1}, \ldots, P_1, p_0) \simeq 1$$

der Fall, d. h. es ist, wie zu beweisen war,

$$(F_1, F_2, \ldots) \simeq 1 .$$

Es ist noch die zweite Hälfte des in § 2 aufgestellten Satzes (I) zu erschließen und demgemäß zu zeigen, daß $(P^{(k)})$ im Bereiche $[[1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m]$ ein Primsystem ist. Daß es kein absolutes Primsystem ist, folgt unmittelbar aus dem Umstande, daß dann auch $(P^{(k+1)})$ in $(P^{(k)})$ enthalten ist.

Werden die Formen von $x_1, \ldots, x_m$ als Formen von $x_{k+1}, \ldots, x_m$ mit Koeffizienten aus $[[1], x_1, \ldots, x_k]$ aufgefaßt, so kann eine solche Form nur dann $\equiv 0 \bmod. (P^{(k)})$ sein, wenn dies für jeden Koeffizienten der Fall ist.

Wäre nun $FG \equiv 0 \left(\bmod. (P^{(k)})\right)$ und trotzdem weder F noch $G \equiv 0 \bmod. (P^{(k)})$, so ließen sich diese Formen in der Gestalt

$$F \equiv A_g x_{k+1}^{g} \cdots x_m^{g} + \cdots,$$

$$G \equiv B_h x_{k+1}^{h} \cdots x_m^{h} + \cdots$$

darstellen, wo die ausgeschriebenen Glieder die „höchsten" sind, deren Koeffizient $\bmod. (l^{(k)})$ von 0 verschieden. Dann wäre aber in FG das höchste Glied

$$A_g B_h x_{k+1}^{g+h} \cdots x_m^{g+h} + \cdots$$

und im Gegensatze zur Annahme $A_g B_h$ nicht $0 \bmod. P^{(k)}$, da dies für keine der beiden dem Bereiche $[[1], x_1, \ldots, x_k]$ angehörenden Formen A_g und B_h stattfindet.

§ 4. Es seien $A_0, A_1, \ldots, A_n$ rationale und ganze Formen von $x_1, \ldots, x_m$ und (S) irgend ein aus ebensolchen Formen bestehendes Divisorensystem; man bezeichnet dann die spezielle diophantische Gleichung, wo A_0 nicht 0 (mod. (S)) ist,

$$A_0 X^n + A_1 X^{n-1} + \cdots + A_n \equiv 0 \pmod{(S)}$$

als „Kongruenz n^{ten} Grades mit einer Unbekannten".

Auf die Theorie der Kongruenzen höheren Grades gehn wir hier nicht ein, da wir von ihr nur den folgenden einfachsten Satz benutzen werden:

Ist (S) ein Primsystem, A_0 nicht 0 (mod. (S)), so kann die Kongruenz

$$A_0 X^n + A_1 X^{n-1} + \cdots + A_n \equiv 0 \pmod{(S)}$$

nicht mehr als n mod. (S) verschiedene Wurzeln besitzen.

Wären nämlich $X_1, \ldots, X_n, X_{n+1}$ solche, so würde aus

$$A_0 X_i^n + A_1 X_i^{n-1} + \cdots + A_n \equiv 0 \pmod{(S)}$$
$$(i = 1, \cdots, n+1)$$

nach den Elementen der Determinantentheorie auch

$$A_0 \,|\, X_i^{j-1} \,| \equiv 0 \pmod{(S)}$$

folgen, wo $|\, X_i^{j-1} \,|$ in bekannter Weise das Differenzenprodukt der X_i bedeutet. Da aber A_0 nicht 0 (mod. (S)) ist, müßten im Gegensatze zur Annahme zwei Größen der Reihe $X_1, \ldots, X_{n+1}$ kongruent 0 (mod. (S)) sein.

Man hat weiter in völliger Analogie mit Kap. II. § 17 den folgenden Satz:

Es seien $F_i(z_1, z_2, \ldots)$, $(i = 1, 2, \ldots)$ Formen, deren Koeffizienten rationale und ganze Formen von $x_1, \ldots, x_m$ sind, und die mod. $(P^{(k)})$, wo $k < m$, von 0 verschieden sind; man kann dann beliebig viele gleichfalls dem Bereiche $[[1], x_1, \ldots, x_m]$ und auch schon dem Bereiche $[[1], x_1, \ldots, x_{k+1}]$ angehörige Größen $\alpha_1, \alpha_2, \ldots$ von der Beschaffenheit bestimmen, daß jedes $F_i(\alpha_1, \alpha_2, \ldots)$ von 0, mod. $(P^{(k)})$, verschieden ist.

Für den Fall einer Unbestimmten z sind in der Reihe $x_{k+1}, x_{k+2}^2, x_{k+1}^3, \ldots$ durchweg mod. $(P^{(k)})$ verschiedene Größen enthalten, von denen, wenn n den Grad von $F(z)$ in z bedeutet, höchstens n der Kongruenz $F(z) \equiv 0$ mod. $(P^{(k)})$ genügen können. Jede andere Größe der angegebenen Reihe genügt also gewiß der aufgestellten Forderung. Der Übergang von $F(z)$ zu $F(z_1, z_2, \ldots)$, sowie zu einer beliebigen Anzahl solcher Formen geschieht alsdann genau ebenso wie an der angeführten Stelle.

Dabei ist aber die Bedingung $k < m$ eine wesentliche, da sonst der Bereich $[[1], x_1, \ldots, x_m]$ ein vollständiges Restsystem mod. $(P^{(m)})$ besitzt, und keine unendliche Reihe inkongruenter Größen mod. $(P^{(m)})$ aufgestellt werden kann. So ist z. B. die Form $x^p - x$ nicht $\equiv 0$ (mod. p) und doch für jede rationale und ganze Zahl a

$$a^p - a \equiv 0 \text{ (mod. } p).$$

Dementsprechend muß auch der Satz von der Transformation einer Form auf die reguläre Gestalt (Kap. II. § 19), wie folgt, modifiziert werden:

Es seien $F_i(z_1, z_2, \ldots, z_r)$, $(i = 1, 2, \ldots)$ irgend welche Formen der Unbestimmten $z_1, z_2, \ldots, z_r$, deren Koeffizienten dem Bereiche $[[1], x_1, \ldots, x_m]$ angehören; dann kann man beliebig viele lineare Transformationen angeben, deren Determinante gleich Eins ist, deren Koeffizienten demselben Bereiche angehören und deren Anwendung die Formen F_i in mod. $(P^{(k)})$ reguläre Formen überführt, wenn wieder $k < m$ ist.

Dabei ist unter einer mod. $(P^{(k)})$ regulären Form wieder eine solche zu verstehn, in welcher, wenn ihre Dimension n ist, die Koeffizienten von $z_1^n, z_2^n, \ldots$ sämtlich (mod. $P^{(k)}$) von 0 verschieden sind.

Ist, ausführlich geschrieben:

$$F_i = \sum_{(g)} A_g^{(i)} z_1^{g_1} z_2^{g_2} \cdots z_r^{g_r}, \qquad (i = 1, \ldots, k)$$

so wird nach Anwendung der folgenden speziellen linearen Transformation

$$z_1 = y_1, \quad z_j = u_{j1} y_1 + y_j, \qquad (j = 2, \ldots, r)$$

deren Determinante gleich Eins ist, wie immer wir uns auch die Bestimmung der u_{j1} vorbehalten, F_i in

$$\overline{F}_i = \sum_{(g)} A_g^{(i)} y_1^{g_1} (u_{21} y_1 + y_2)^{g_2} \cdots (u_{r1} y_1 + y_r)^{g_r}$$

übergehn, wo der Koeffizient von y_1^n gleich

$$\Sigma A_g^{(i)} u_{21}^{g_2} \ldots u_{r1}^{g_r},$$

wenn die Summation über alle jene Glieder ausgedehnt wird, für die $g_1 + g_2 + \cdots + g_r = n$ ist.

Wie eben bewiesen wurde, können die Größen $u_{21}, \ldots, u_{r1}$ allerdings nicht immer als rationale und ganze Zahlen, wohl aber schon als Formen des Bereichs $[[1], x_1, \ldots, x_{k+1}]$ so gewählt werden, daß der Koeffizient von y_1^n von 0 mod. $(P^{(k)})$ verschieden wird, während $y_2^n, \ldots$ in $\overline{F}_i$ dieselben Koeffizienten besitzen, wie $z_2^n, \ldots$ in F_i.

Die Fortsetzung dieses Verfahrens ergibt endlich, genau ebenso wie in Kap. II. § 18, lineare Transformationen, die den oben ausgesprochenen Bedingungen genügen, und nach deren Anwendung die Formen $F_i(z_1, z_2, \ldots)$ in solche Formen $\overline{F}_i(\bar{z}_1, \bar{z}_2, \ldots)$ übergehn, die mod. $(P^{(k)})$ in Bezug auf alle Unbestimmte $\bar{z}_1, \bar{z}_2, \ldots$ regulär sind.

Um für die Theorie der Teilbarkeit der rationalen und ganzen Formen auch formal eine völlig einheitliche Darstellung zu gewinnen, wird es angezeigt sein, das Symbol $(P^{(-1)})$ einzuführen, unter dem man auch die Null verstehn kann. Die Aussage $F_1 \equiv F_2 \pmod{(P^{(-1)})}$ soll dann einfach $F_1 = F_2$ bedeuten.

Die „Theorie der rationalen und ganzen Formen mod. $(P^{(k)})$" enthält dann für $k = -1$ auch die früher entwickelten Sätze.

Divisorensysteme mod. $(P^{(k)})$.

§ 5. In Erweiterung unsrer früheren Festsetzungen erhalten wir die folgenden Definitionen:

I. Das Divisorensystem $(M_1, \ldots, M_h)$ „enthält mod. $(P^{(k)})$" das Divisorensystem $(N_1, \ldots, N_g)$, wenn für jedes Element des ersten Divisorensystems die Kongruenz

$$M_i \equiv 0 \ \left(\text{mod. } N_1, \ldots, N_g, (P^{(k)})\right)$$

besteht.

II. Zwei Divisorensysteme heißen (im engeren Sinne) äquivalent mod. $(P^{(k)})$, wenn jedes von ihnen das andere mod. $(P^{(k)})$ enthält. In Zeichen soll dies durch

$$(M_1, \ldots, M_h) \simeq (N_1, \ldots, N_g) \ \left(\text{mod. } (P^{(k)})\right)$$

ausgedrückt werden. Es genügen übrigens dazu auch schon die bisherigen Bezeichnungen, denn die Äquivalenz

$$\left(M_1, \ldots, M_h, (P^{(k)})\right) \simeq \left(N_1, \ldots, N_g, (P^{(k)})\right)$$

besagt, wie man unmittelbar sieht, genau dieselbe Tatsache.

Es wird auch hier die soeben definierte engere Äquivalenz von der weiteren Äquivalenz, die durch das Zeichen $\sim$ angedeutet wird, zu unterscheiden sein. Es ist

$$(M_1, \ldots, M_h) \sim (N_1, \ldots, N_g) \text{ mod. } (P^{(k)}),$$

wenn jeder gemeinschaftliche Teiler mod. $(P^{(k)})$ von $M_1, \ldots, M_h$ auch ein gemeinschaftlicher Teiler mod. $(P^{(k)})$ von $N_1, \ldots, N_g$ ist und umgekehrt.

Für einzelne Größen (eingliedrige Divisorensysteme) fallen die beiden Aussagen

$$M \sim N \ \left(\text{mod. } (P^{(k)})\right) \text{ und } M \simeq N \ \left(\text{mod. } (P^{(k)})\right)$$

wieder zusammen.

Man wird dann ebenso wie in Kap. VII. § 2 den „größten gemeinschaftlichen Inhalt mod. $(P^{(k)})$" zweier Divisorensysteme definieren und auch die Divisorensysteme $(M_1, \ldots, M_h)$

und $(N_1, \ldots, N_g)$ „relativ prim mod. $(P^{(k)})$“ nennen, wenn

$$(M_1, \ldots, M_h, N_1, \ldots, N_g) \simeq 1 \ (\text{mod. } (P^{(k)}),$$

oder also

$$\left(M_1, \ldots, M_h, N_1, \ldots, N_g, (P^{(k)})\right) \simeq 1$$

ist.

Auch die Entwicklungen in Kap. VII. § 3 bleiben Wort für Wort gültig, wenn man statt der dort angewandten Äquivalenz schlechtweg Äquivalenzen mod. $(P^{(k)})$ versteht, und man hat insbesondere den wichtigen Satz:

III. Ist in dem Divisorensystem $(N_1, \ldots, N_g)$ nicht jedes Element $\equiv 0$ (mod. $(P^{(k)})$, und

$$(\ldots, M_i, \ldots)(\ldots, N_j, \ldots) \simeq (\ldots, M_{i'}', \ldots)(\ldots, N_j, \ldots) \left(\text{mod.}(P^{(k)})\right),$$
$$(i = 1, \ldots, h;\ i' = 1, \ldots, h';\ j = 1, \ldots, g),$$

so enthält mod. $(P^{(k)})$ das Divisorensystem $(\ldots, M_i^g, \ldots)$ das System $(\ldots, M_i', \ldots)$ und $(\ldots, M_{i'}^g, \ldots)$ auch $(\ldots, M_i, \ldots)$.

Wenn wir nun solche Formen betrachten, deren Koeffizienten dem Bereiche

$$[[1], x_1, \ldots, x_m] \ (\text{mod. } P^{(k)})$$

angehören, so bleiben, wie schon erwähnt, die auf den Kroneckerschen Fundamentalsatz bezüglichen Entwicklungen in § 5—8 des dritten Kapitels unbedingt gültig, sobald nur an Stelle des Zeichens „=“ jetzt die Kongruenzbezeichnung mod. $(P^{(k)})$ gesetzt wird; es ist dabei nur zu beachten, daß wegen der so festgelegten Bedeutung der Unbestimmten $x_1, \ldots, x_m$ statt der dort gebrauchten Bezeichnung die Unbestimmten der Formen jetzt anders, z. B. mit $z_1, \ldots, z_n$ bezeichnet werden müssen. Ebenso setzen wir $Q_1, \ldots, Q_i, \ldots$ für die früher gebrauchten Buchstaben $P_1, \ldots, P_i, \ldots$, die jetzt die Elemente des Divisorensystems $(P^{(k)})$ bedeuten. Man hat dann in Analogie mit dem zu Beginn des § 6 in Kap. III ausgesprochenen Satze die folgende weitgehende Verallgemeinerung des Kroneckerschen Fundamentalsatzes:

IV. Es seien

$$F_j \equiv \sum_{(g)} A_g^{(j)} z_1^{g_1} \dots z_n^{g_n} \left(\text{mod. } (P^{(k)})\right) \qquad (j = 1, 2, \dots, h)$$

mod. $(P^{(k)})$ von 0 verschiedene Formen der Unbestimmten $z_1, \dots, z_n$, deren Koeffizienten dem pseudoholoiden Bereiche $[[1], x_1, \dots, x_m]$ $\left(\text{mod. } (P^{(k)})\right)$ angehören, und das Produkt dieser Formen

$$F \equiv F_1 \dots F_h \equiv \sum C_g z_1^{g_1} \dots z_n^{g_n} \left(\text{mod. } (P^{(k)})\right);$$

es sei ferner

$$Q_i = A_{i_1}^{(1)} A_{i_2}^{(2)} \dots A_{i_h}^{(h)}$$

das Produkt von h solchen Koeffizienten, deren jeder einer anderen Form F_j entnommen ist.

Dann gibt es eine Reihe von Größen $H_1, \dots, H_\nu$, die mod. $(P^{(k)})$ von 0 verschiedene rationale und ganze, homogene Formen der Koeffizienten $A^{(1)}, \dots, A^{(h)}$ sind, und eine weitere Reihe von Größen $L_{i\sigma}^{(s)}$, die rationale und ganze, homogene und lineare Formen der Größen C_g sind, so daß

$$H_s Q_i \equiv \sum_{\sigma=1}^{\nu} L_{i\sigma}^{(s)} H_\sigma \left(\text{mod. } (P^{(k)})\right), \qquad (s = 1, \dots, \nu) \qquad \text{(K)}$$

wird.

Da der Bereich $[[1], x_1, \dots, x_m]$ $\left(\text{mod. } (P^{(k)})\right)$ ein vollständiger pseudoholoider Bereich ist, sind auch die weiteren Schlüsse in Kap. III. § 8 anwendbar, und man hat

$$(Q_1, \dots, Q_i, \dots) \sim (C_1, \dots, C_g, \dots) \left(\text{mod. } (P^{(k)})\right),$$

d. h. der größte gemeinschaftliche Teiler mod. $(P^{(k)})$ der Formenreihen $(Q_1, \dots, Q_i, \dots)$ und $(C_1, \dots, C_g, \dots)$ ist derselbe.

Der Kroneckersche Fundamentalsatz ist aber noch in anderer Richtung zu erweitern, wenn man nämlich versucht, in der Fragestellung, wie dies nach der Einführung der Divisorensysteme von selbst geboten erscheint, von der weiteren Äquivalenz der Divisorensysteme $(Q_1, \dots, Q_i, \dots)$ und $(C_1, \dots, C_g, \dots)$ zu ihrer engeren Äquivalenz aufzusteigen. Eine solche findet allerdings nicht statt, denn $(C_1, \dots, C_a, \dots)$

enthält zwar das Divisorensystem $(Q_1, \ldots, Q_i, \ldots)$; umgekehrt hat man aber nur den folgenden trotz seiner Beschränkung grundlegenden Satz:

V. Es gibt eine positive ganze Zahl ν von der Beschaffenheit, daß

$$(Q_1^\nu, \ldots, Q_i^\nu, \ldots)$$

mod. $(P^{(k)})$ das Divisorensystem $(C_1, \ldots, C_g, \ldots)$ enthält.

Der Satz ergibt sich unmittelbar aus den Kongruenzen (K), wenn man den in diesem Paragraphen angeführten Satz (III) benutzt.

Nach der Bedeutung der Formen $L_{i\,\sigma}^{(s)}$ enthält mod. $(P^{(k)})$ das Divisorensystem $(\ldots, H_s Q_i, \ldots)$ das Divisorensystem $(\ldots, H_s C_g, \ldots)$, und auch $(\ldots, H_s C_g, \ldots)$ das System $(\ldots, H_s Q_i, \ldots)$. Beides sind aber komponierte Systeme, und man hat, wenn wir sie als Produkt ihrer Kompositionsfaktoren schreiben,

$$(\ldots, H_s, \ldots)(\ldots, Q_i, \ldots) \simeq (\ldots, H_s, \ldots)(\ldots, C_g, \ldots) \left(\text{mod.}\,(P^{(k)})\right).$$

Hieraus ergibt sich aber nach (III) unmittelbar der ausgesprochene Satz.

Theorie der Resolventenformen mod. $(P^{(k)})$.

§ 6. Um die in Kap. III. § 18 entwickelte Theorie der Resolventenform eines Formensystems $F_1, F_2, \ldots, F_h$ genau und ohne jede Änderung auf die Formen des Bereichs

$$[[1], x_1, \ldots, x_m] \left(\text{mod.}\,(P^{(k)})\right)$$

anwenden zu können, werden wir die Formen F als Formen der Unbestimmten $x_{k+2}, \ldots, x_m$ ansehn, deren Koeffizienten dem Bereiche $[[1], x_1, \ldots, x_k, x_{k+1}] \left(\text{mod.}\,(P^{(k)})\right)$ angehören. Da dieser Bereich noch unendlich viele nicht kongruente Formen enthält, wird es immer beliebig viele lineare Transformationen geben, deren Determinante $\not\equiv 1$, und deren Koeffizienten dem pseudoholoiden Bereiche $[[1], x_1, \ldots, x_k, x_{k+1}]$ angehören, für welche beliebig viele Formen F zugleich regulär in Bezug auf $x_{k+2}, \ldots, x_m$ werden.

Die Analogie mit dem an der angeführten Stelle allein behandelten Falle $k = -1$ ist dann eine vollständige, wenn man nur berücksichtigt, daß an Stelle der rationalen ganzen Zahlen jetzt die Formen des Bereichs

$$[[1], x_1, \ldots, x_k, x_{k+1}] \ \left(\text{mod. } (P^{(k)})\right)$$

treten

Dabei wird der Fall, daß die Formen F die Unbestimmten $x_{k+2}, \ldots, x_m$ überhaupt nicht enthalten, als besonders einfach, zuerst zu behandeln sein. Die Formen mögen in diesem Falle mit

$$f_j(x_1, \ldots, x_k, x_{k+1}) \ \left(\text{mod. } (P^{(k)})\right)$$

bezeichnet werden.

Ist der größte gemeinschaftliche Teiler von

$$f_1, \ldots, f_h \ \left(\text{mod. } (P^{(k)})\right)$$

z. B. $\sim d$, also

$$f_j \equiv d f_j' \ \left(\text{mod. } (P^{(k)})\right)$$

und

$$(f_1', \ldots, f_h') \sim 1 \ \left(\text{mod. } (P^{(k)})\right),$$

so ist

$$d \sum_{j=1}^{h} f_j' w_j \equiv 0 \ (\text{mod. } f_1, \ldots, f_h, P^{(k)})$$

„die Resolventenform von $f_1, \ldots, f_h \ \left(\text{mod. } (P^{(k)})\right)$“.

Dabei mag sogleich bemerkt werden, daß die Frage nach der Lösbarkeit der Kongruenz

$$\sum_{j=1}^{h} f_j X_j \equiv 1 \ \left(\text{mod. } (P^{(k)})\right),$$

sowie die Bestimmung einer Lösung davon, wenn sie überhaupt lösbar ist, schon hier erledigt werden kann. (Für $k = -1$ hat man es also mit einer Gleichung zu tun, in der die Koeffizienten sämtlicher Unbekannten rationale und ganze Zahlen sind.)

Die notwendige und hinreichende Bedingung der Lösbarkeit jener Gleichung ist

$$(f_1, \ldots, f_h) \sim 1 \ \left(\text{mod. } (P^{(k)})\right),$$

wo, da das weitere Äquivalenzzeichen ~ 1 angewandt wird, $(f_1, \ldots, f_h)$ den größten gemeinschaftlichen Teiler von $f_1, \ldots, f_h$ bedeutet.

Wir erkennen diese Bedingung unmittelbar als notwendig, da mit $f_1, \ldots, f_h$ auch $\Sigma f_j X_j = 1$ durch jenen größten gemeinschaftlichen Teiler $\left(\text{mod. } (P^{(k)})\right)$ teilbar sein muß. Dieser ist daher ein Teiler der Einheit mod. $(P^{(k)})$ und demnach

$$\sim 1 \ (\text{mod. } P^{(k)}).$$

Daß diese Bedingung auch hinreichend ist, erkennen wir, indem wir in diesem Falle durch die folgende Reduktionsmethode eine Lösung wirklich angeben.

Wenn einer der Koeffizienten, z. B. f_1, die Unbestimmte x_{k+1} überhaupt nicht enthält, so gibt es, da wir ja nur mod. $(P^{(k)})$ von Null verschiedene Koeffizienten annehmen können, eine zweite leicht zu bestimmende Form $g(x_1, \ldots, x_k)$, die wieder mod. $(P^{(k)})$ von Null verschieden ist und $f_1 g \equiv 1$ ergibt. Die Kongruenz geht aber durch Multiplikation mit g in die gleichwertige Gestalt

$$X_1 + \sum_{j=2}^{h} f_j g X_j \equiv g \ \left(\text{mod. } (P^{(k)})\right)$$

über, deren allgemeine Lösung

$$X_1 \equiv g - \sum_{j=2}^{h} f_j g t_j, \ X_j \equiv t_j, \ (j = 2, \ldots, h)$$

ist, wo $t_2, \ldots, t_h$ beliebige Formen bedeuten.

(Im Falle $k = -1$, wo die Koeffizienten überhaupt keine Unbestimmten enthalten, entspricht diesem Ausnahmefalle die „gelöste" Form der Kongruenz, wo ein Koeffizient schon gleich Eins ist.)

Enthalten alle Koeffizienten die Unbestimmte x_{k+1}, wo wir wieder zuerst den Fall $k = -1$ ausschließen, so wird der Grad eines f, z. B. f_1, in x_{k+1} nicht größer sein, als der irgend eines andern f_j. Setzt man dann

$$f_j \equiv f_1 q_j + r_j \ \left(\text{mod. } (P^{(k)})\right),$$

wo q_j und r_j der Quotient und Rest sind, die bei dem gewöhnlichen Divisionsverfahren auftreten, so werden, da die Division mod. $(P^{(k)})$ ausgeführt wird, q_j und r_j wieder rationale und ganze Formen sein, dabei aber ist der Grad von r_j mindestens um Eins niedriger als der von f_1, oder aber

$$r_j \equiv 0 \ \left(\text{mod. } (P^{(k)})\right).$$

Die Kongruenz kann dann in der Gestalt

$$f_1(X_1 + q_2 X_2 + \cdots + q_h X_h) + \sum_{j=2}^{h} r_j X_j \equiv 1 \ \left(\text{mod. } (P^{(k)})\right)$$

geschrieben werden und ist demnach mit der Kongruenz

$$f_1 Y_1 + \sum_{j=2}^{h} r_j X_j \equiv 1 \ \left(\text{mod. } (P^{(k)})\right)$$

zugleich gelöst. Für diese ist der größte gemeinschaftliche Teiler der Koeffizienten wieder

$$(f_1, r_2, \ldots, r_h) \sim (f_1, f_2, \ldots, f_h) \sim 1,$$

und also, da der Annahme nach f_1 nicht $\equiv 1$ ist, ein r gewiß von 0 verschieden. War der Grad von f_1 in x_{k+1} gleich n, so gelangt man demnach bei Anwendung dieser Reduktionsmethode nach höchstens n Schritten zu einer Kongruenz, in der ein Koeffizient von x_{k+1} unabhängig ist, deren Lösung mithin unmittelbar hingeschrieben werden kann.

(Für den elementaren Ausnahmefall $k = -1$ sind die Koeffizienten rationale und ganze Zahlen, die durch das angegebene Verfahren nicht dem Grade, sondern der absoluten Größe nach reduziert werden. War der kleinste Koeffizient — vom Vorzeichen abgesehn — n, so gelangt man nach höchstens n Schritten zu einer Gleichung, in welcher ein Koeffizient ± 1 ist, deren Lösung also wieder unmittelbar hingeschrieben werden kann.)

§ 7. Für die allgemeine Aufstellung der Resolventenform mod. $(P^{(k)})$ des Formensystems $F_1, \ldots, F_h$ sind nun die Entwicklungen in Kap. III. § 18 zu wiederholen. Sie

gelten Wort für Wort, wenn man nur an Stelle der „rationalen und ganzen Zahlen" überall „rationale und ganze Formen von $x_1, \ldots, x_{k+1}$ $\left(\text{mod. } (P^{(k)})\right)$", und ebenso in der Kongruenzbeziehung an Stelle des Modulsystems $(F_1, F_2, \ldots)$ nun $\left(F_1, F_2, \ldots, F_h, (P^{(k)})\right)$ setzt. Die Reihe der Unbestimmten endlich ist jetzt nicht $x_1, \ldots, x_m$, sondern $x_{k+2}, \ldots, x_m$.

Man gelangt somit zur Resolventenform mod. $(P^{(k)})$ des Formensystems $F_1, \ldots, F_h$:

$$D D^{(1)} \ldots D^{(r)} \sum_{j_r=1}^{k_r} C_{j_r} w_{j_r} \equiv 0 \left(\text{mod. } F_1, \ldots, F_h, (P^{(k)})\right), \quad \text{(R)}$$

wo $D^{(r)}, C_{j_r}$ dem Bereiche $[[1], x_1, \ldots, x_{k+1}]$ $\left(\text{mod. } (P^{(k)})\right)$ angehören, $r \leqq m - k - 1$ ist, und allgemein $D^{(s)}$ eine diesem Bereiche entstammende Form von $x_{s+k+2}, \ldots, x_m$ ist. D (oder $D^{(0)}$) ist der größte gemeinschaftliche Teiler mod. $(P^{(k)})$ von $F_1, \ldots, F_h$.

Dabei können die Formen D durchweg als regulär in Bezug auf $x_{k+2}, \ldots, x_m$ angenommen werden, da dies durch eine bekannte lineare Transformation mit dem Bereiche $[[1], x_1, \ldots, x_{k+1}]$ $\left(\text{mod. } (P^{(k)})\right)$ angehörigen Koeffizienten, die auf das Formensystem $F_1, \ldots, F_h$ anzuwenden ist, immer erreicht werden kann. Die Kongruenz (R) bleibt übrigens auch dann gültig, wenn wir diese lineare Transformation nicht anwenden, nur werden dann die D nicht immer regulär sein.

Die Größen C_{j_r} gehören dem Bereiche

$$[[1], x_1, \ldots, x_k, x_{k+1}] \left(\text{mod. } (P^{(k)})\right)$$

an; sei ihr größter gemeinschaftlicher Teiler mod. $(P^{(k)})$:

$$(\ldots, C_{j_r}, \ldots) \sim D^{(r+1)} \left(\text{mod. } (P^{(k)})\right),$$

so kann man, wie bewiesen, die Größen w_{j_r} der Bedingung

$$\sum_{j_r=1}^{k_r} C_{j_r} w_{j_r} \equiv D^{(r+1)} \left(\text{mod. } (P^{(k)})\right)$$

gemäß bestimmen und erhält damit die für den vorliegenden Fall vereinfachte Resolventenform:

$$DD^{(1)} \dots D^{(r)} D^{(r+1)} \equiv 0 \ \left(\text{mod. } F_1, \dots, F_h, (P^{(k)})\right). \qquad (R_k)$$

Der so hergestellte Ausdruck liefert die Grundlage für die Untersuchung derjenigen P-Systeme, die in $\left(F_1, \dots, F_h, (P^{(k)})\right)$ oder, was dasselbe ist, in $(F_1, \dots, F_h)$ und $(P^{(k)})$ enthalten sind. Ohne diese Theorie in voller Allgemeinheit zu verfolgen, sollen hier nur die für unsre Zwecke notwendigen Sätze abgeleitet werden.

Jedes in $P^{(k)}$ enthaltene P-System kann so geschrieben werden, daß seine letzten $k+1$ Elemente mit den Elementen von $(P^{(k)})$ geradezu übereinstimmen.

Die vereinfachte Resolventenform ist nun entweder $\simeq 1 \left(\text{mod. } (P^{(k)})\right)$, oder sie kann in ihre mod. $(P^{(k)})$ irreduzibeln Faktoren zerlegt werden, und es sei dann:

$$DD^{(1)} \dots D^{(r)} D^{(r+1)} \simeq E_1^{a_1} \dots E_s^{a_s} \ \left(\text{mod. } (P^{(k)})\right).$$

Jedes der gesuchten P-Systeme muß als Primsystem in einer der Formen E enthalten sein. Wir betrachten nun erstens den Fall, wo irgend einer der Faktoren E eine wirkliche Form der Unbestimmten $x_{k+2}, \dots, x_m$ mit Koeffizienten aus $[[1], x_1, \dots, x_{k+1}] \left(\text{mod. } (P^{(k)})\right)$ ist.

Es zeigt sich dann zuerst, daß in

$$E(x_{k+2}, \dots, x_m)$$

für $x_{k+2}, \dots, x_m$ solche Größen $\xi_{k+2}, \dots, \xi_m$ des Bereichs $[[1], x_1, \dots, x_{k+1}] \left(\text{mod. } (P^{(k)})\right)$ gesetzt werden können, daß

$$E(\xi_{k+2}, \dots, \xi_m) \equiv 0 \ \text{mod.} \left(\pi_{k+1}, (P^{(k)})\right)$$

wird, wo π_{k+1} eine irreduzible Form des angegebenen Bereichs ist, die von den irgendwie gegebenen irreduzibeln Formen $\pi', \pi'', \dots, \pi^{(s)}$ desselben Bereichs verschieden ist.

Wenn α das von den Unbestimmten $x_{k+2}, \ldots, x_m$ unabhängige Glied*) der Form E ist, setzen wir

$$x_{k+r} = \alpha\pi' \cdots \pi^{(s)} z_{k+r} \cdots, \qquad (r = 2, \cdots, m - k).$$

Dann ist

$$\frac{1}{\alpha} E(\alpha\pi' \cdots \pi^{(s)} z_{k+2}, \cdots, \alpha\pi' \cdots \pi^{(s)} z_m)$$

mod. $(P^{(k)})$ bei keinem Werte von $z_{k+1}, \ldots, z_m$ durch irgend ein $\pi^{(i)}$ teilbar; denn dieser Ausdruck ist, wie unmittelbar zu sehen,

$$\equiv 1 \left(\text{mod. } \pi^{(i)}, (P^{(k)})\right).$$

Man kann aber nach § 4 dieses Kapitels die Größen z aus dem Bereiche $[[1], x_1, \ldots, x_{k+1}]$ $\left(\text{mod. } (P^{(k)})\right)$ so bestimmen, daß keine der Formen

$$\frac{1}{\alpha} E(\alpha\pi' \cdots \pi^{(s)} z_{k+2}, \cdots, \alpha\pi' \cdots \pi^{(s)} z_m) - C_j$$

mod. $(P^{(k)})$ verschwindet, wo C_j irgend ein Element des vollständigen Restsystems der Formen $[[1], x_1, \ldots, x_k]$ $\left(\text{mod. } (P^{(k)})\right)$ bedeutet. In diesem Falle wird also $\frac{1}{\alpha} E(\alpha\pi' \ldots \pi^{(s)} z_{k+2}, \ldots)$ eine wirkliche Form der Unbestimmten $x_{k+1}, \ldots, x_m$, mithin auch durch eine irreduzible Form π_{k+1} teilbar, die von $\pi', \ldots, \pi^{(s)}$ verschieden sein muß. Dasselbe wird, wie behauptet, für E der Fall sein.

Es sei nun E in dem Faktor $D^{(i)}$ der Resolventenform enthalten, also eine Form von $x_{k+i+2}, \ldots, x_m$; die Reihe $\pi', \ldots, \pi^{(s)}$ umfasse alle irreduzibeln Formen, die in den Koeffizienten der höchsten Glieder der Formen $F_{j_h}^{(h)}$ (nach der Bezeichnung in Kap. III. § 18) vorkommen. Dann wird nach dem eben hergeleiteten Satze:

$$E \equiv 0 \left(\text{mod. } x_{k+i+2} - \xi_{k+i+2}, \cdots, x_m - \xi_m, \pi_{k+1}, (P^{(k)})\right).$$

*) Der Fall $\alpha = 0$ kann durch eine einfache Transformation immer vermieden werden.

Das hierin stehende Modulsystem ist ein P-System, in dem, wenn $i > 0$, die Unbestimmten $x_{k+2}, \ldots, x_{k+i+1}$ noch nicht zur Verwendung kommen.

Ist $i = 0$, also E ein Teiler von D, d. h. auch ein Teiler aller F, so gibt es demnach unendlich viele P-Systeme $(P^{(m)})$, die in allen F enthalten sind.

Ist $i > 0$, E ein Teiler von $D^{(i)}$, und also (wieder in den Bezeichnungen des Kap. III. § 18) $D^{(i)}$ der größte gemeinschaftliche Teiler mod. $(P^{(k)})$ von $F_1^{(i)}, F_2^{(i)}, \ldots$, so sind auch diese Formen

$$\equiv 0 \left(\text{mod. } x_{k+i+2} - \xi_{k+i+2}, \ldots, x_m - \xi_m, \pi_{k+1}, (P^{(k)})\right).$$

Es haben demnach die Formen $\overline{F}^{(i-1)}$ einen größten gemeinschaftlichen Teiler nach jenem Modulsysteme, der eine neue Unbestimmte x_{k+i+1} und nur eine solche enthält. Wählt man irgend einen irreduzibeln Teiler von ihnen, z. B. P_{k+i+1}, so wird auch für jedes $F^{(i-1)}$

$$F^{(i-1)} \equiv 0 \left(\text{mod. } P_{k+i+1}, x_{k+i+2} - \xi_{k+i+2}, \ldots, \pi_{k+1}, (P^{(k)})\right).$$

Da man in dieser Weise bis zu den Formen F zurückschließen kann, gelangt man zu dem wichtigen Resultate, daß das Formensystem

$$\left(F_1, \ldots, F_h, (P^{(k)})\right)$$

unendlich viele P-Systeme $m + 1^{\text{ter}}$ Stufe enthält, sobald in der Resolventenform auch nur eine der Unbestimmten $x_{k+2}, \ldots, x_m$ wirklich vorkömmt.

Ist zweitens die Resolventenform, also auch jeder Faktor E eine Form der einzigen Unbestimmten x_{k+1}, selbstverständlich mit Koeffizienten aus $[[1], x_1, \ldots, x_k]$ $\left(\text{mod. } (P^{(k)})\right)$, so ist

$$E \simeq x_{k+1}^{n_{k+1}} + \cdots \left(\text{mod. } (P^{(k)})\right)$$

und kann geradezu als P_{k+1} geschrieben werden. Setzt man daher

$$(P^{(k+1)}) \simeq \left(P_{k+1}, (P^{(k)})\right),$$

so müssen die gesuchten P-Systeme in einem der so bestimmten Systeme

$$\left(F_1, \ldots, F_h, (P^{(k+1)})\right)$$

enthalten sein, und es ist umgekehrt jedes in diesem Systeme enthaltene P-System auch in $\left(F_1, \ldots, F_h, (P^{(k)})\right)$ enthalten. Damit ist aber eine Reduktion des Problems gegeben, und man erhält die in $\left(F_1, \ldots, F_h, (P^{(k)})\right)$ enthaltenen P-Systeme $m + 1^{\text{ter}}$ Stufe, nach höchstens $m - k$-maliger Wiederholung dieses Verfahrens, als die in einer endlichen Reihe von Systemen der Gestalt

$$\left(F_1, \ldots, F_h, (P^{(m)})\right)$$

enthaltenen P-Systeme, falls nicht bei den reduzierten Systemen irgendwo der erste Fall eintritt, mithin eine unendliche Anzahl von P-Systemen $m + 1^{\text{ter}}$ Stufe vorhanden ist, die der gestellten Bedingung genügen.

Ist dies niemals der Fall gewesen, so wird endlich jedes F als Form von $x_1, \ldots, x_m$ entweder $\equiv 0 \left(\text{mod. } (P^{(m)})\right)$, oder $\simeq 1 \left(\text{mod. } (P^{(m)})\right)$. Ist auch nur für ein F das letztere der Fall, so wird

$$\left(F_1, \ldots, F_h, (P^{(m)})\right) \simeq 1,$$

und man erhält schließlich die in $\left(F_1, \ldots, F_h, (P^{(k)})\right)$ enthaltenen P-Systeme $m + 1^{\text{ter}}$ Stufe in der endlichen Reihe jener $(P^{(m)})$, für die

$$F_j \equiv 0 \ (\text{mod. } P^{(m)}), \qquad (j = 1, \ldots, h)$$

ist.

Ist endlich für jedes $(P^{(m)})$

$$\left(F_1, \ldots, F_h, (P^{(m)})\right) \simeq 1,$$

so wird, da die Resolventenformen von $F_1, \ldots, F_h$ nach irgend einem $(P^{(m-1)})$ einem Potenzenprodukte gewisser $P^{(m)}$ äquivalent ist, auch für jedes in Frage kommende $(P^{(m-1)})$:

$$\left(F_1, \ldots, F_h, (P^{(m-1)})\right) \simeq 1,$$

und indem man so zurückschließt, endlich auch

$$\left(F_1, \ldots, F_h, (P^{(k)})\right) \simeq 1.$$

§ 8. Die Theorie der Resolventenform mod. $(P^{(k)})$ führt auch schon auf Grundlage der hier ausgeführten einfachsten Sätze zu wichtigen Schlußfolgerungen. So erhalten wir aus dem Vorstehenden unmittelbar einen Beweis für den schon in § 2 angeführten Satz, daß die P-Systeme $m+1^{\text{ter}}$ Stufe die Gesamtheit der im Bereiche der rationalen und ganzen Formen von m Unbestimmten vorhandenen absoluten Primsysteme und nur diese ergeben.

Soll nämlich $(F_1, \ldots, F_h)$ ein absolutes Primsystem (und demnach auch nicht $\simeq 1$) sein, so erhält man nach den ausgeführten Entwicklungen immer ein System $(P^{(m)})$, das in $(F_1, \ldots, F_h)$ enthalten ist. Es muß also, wenn dieses System ein absolutes Primsystem sein soll, in der Tat

$$(F_1, \ldots, F_h) \simeq (P^{(m)})$$

sein.

Ferner ergibt sich aus den dargelegten Sätzen unmittelbar die Lösung des zweiten Fundamentalproblems in der arithmetischen Theorie der linearen diophantischen Gleichungen. Als solches wurde in § 1. des Kap. VII. das folgende formuliert:

Entscheidung der Lösbarkeit für eine lineare diophantische Gleichung der Gestalt:

$$\Sigma F_i X_i = 1 \tag{1}$$

und Bestimmung einer Lösung, wenn eine solche vorhanden ist.

Wir schreiben die zu untersuchende Gleichung nur formell allgemeiner:

$$\sum_{i=1}^{h} F_i X_i \equiv 1 \ \left(\text{mod. } (P^{(k)})\right), \tag{2}$$

eine Kongruenz, die für $k = -1$ in die oben angeführte Gleichung übergeht. Wenn diese Kongruenz eine Lösung besitzt, so ist

$$(F_1, \ldots, F_h) \simeq 1 \ \left(\text{mod. } (P^{(k)})\right),$$

eine Äquivalenz, die unmittelbar als notwendige und hinreichende

Bedingung für die Lösbarkeit jener Kongruenz anzusehn ist. Dann muß vor allem die Resolventenform mod. $(P^{(k)})$ von $F_1, \ldots, F_h$ eine Form von x_{k+1} allein sein mit Koeffizienten aus $[[1], x_1, \ldots, x_k]$ $\left(\text{mod. } (P^{(k)})\right)$. Enthält diese auch x_{k+1} nicht, so ist sie $\simeq 1$ mod. $(P^{(k)})$ und wird nach Multiplikation mit einer unmittelbar zu bestimmenden Größe $\equiv 1$ $\left(\text{mod. } (P^{(k)})\right)$. Die Berechnung der Resolventenform nach dem angegebenen Verfahren ergibt aber für diese auch eine Darstellung als lineare Form der F mit bekannten Koeffizienten und demnach schließlich die identische Kongruenz

$$\Sigma F_i \lambda_i \equiv 1 \pmod{P^{(k)}},$$

d. h. eine Lösung von (2).

Enthält die Resolventenform die Unbestimmte x_{k+1}, so ist sie

$$\sim P_{k+1,1}^{a_1} \cdots P_{k+1,s}^{a_s} \left(\text{mod. } (P^{(k)})\right),$$

wo jedes $P_{k+1,\nu}$ von der Gestalt $x_{k+1}^{\nu r} + \cdots$ ist. Es ist dann aber auch

$$\left(F_1, \ldots, F_h, P_{k+1,1}^{a_1} \cdots P_{k+1,s}^{a_s}\right) \simeq (F_1, \ldots, F_h) \simeq 1 \left(\text{mod. } (P^{(k)})\right).$$

Dann muß auch

$$(F_1, \ldots, F_h, P_{k+1,r}) \simeq 1 \left(\text{mod. } (P^{(k)})\right)$$

sein, da ein in diesem enthaltenes absolutes Primsystem auch in $(F_1, \ldots, F_h)$ enthalten ist. Diese Äqnivalenz läßt sich in der Gestalt

$$(F_1, \ldots, F_h) \simeq 1 \left(\text{mod. } P_{k+1,r}, (P^{(k)})\right)$$

schreiben und ergibt eine Reduktion des Problems (2) auf das Problem der Kongruenz

$$\sum_{i=1}^{h} F_i X_i \equiv 1 \left(\text{mod. } P_{(r)}^{(k+1)}\right) \qquad (r = 1, \ldots, s), \qquad (3)$$

wenn wir für das als Modulsystem verwendete P-System dieses kürzere Symbol benützen. Unter der Voraussetzung, daß die

Theorie dieser Kongruenz vollständig erledigt ist, ist auch das ursprüngliche Problem gelöst. Denn (2) hat, wie soeben gezeigt wurde, nur dann eine Lösung, wenn dies für die Kongruenzen (3) der Fall ist; andrerseits läßt sich aber, wenn jene Lösung jeder einzelnen Kongruenz (3) bekannt ist, eine Lösung von (2) direkt angeben.

Die Lösungen von (3) seien durch die folgenden identischen Kongruenzen charakterisiert:

$$\sum_{i=1}^{h} F_i \mu_{ir} \equiv 1 \ \left(\text{mod. } P_{k+1,r}, (P^{(k)})\right); \quad (r = 1, \ldots, s)$$

man kann diese dann auch in der Gestalt

$$\sum_{i=1}^{h} F_i \mu_{ir} + P_{k+1,\nu} \nu_r \equiv 1 \ \left(\text{mod. } (P^{(k)})\right) \quad (r = 1, \ldots, s)$$

schreiben, da für gegebene μ eine Darstellung von $\sum_{i=1}^{h} F_i \mu_{ir} - 1$, als homogene lineare Form der Elemente von $\left(P^{(k+1)}_{(\nu)}\right)$ durch das gewöhnliche Divisionsverfahren gegeben wird.

Wenn man diese identische Kongruenz zur a_r^{ten} Potenz erhebt und passend ordnet, erhält man hieraus wieder eine identische Relation der Gestalt

$$\sum_{i=1}^{h} F_i \mu'_{ir} + P^{a_r}_{k+1,\nu} \nu_r^{a_r} \equiv 1 \ \left(\text{mod. } (P^{(k)})\right) \quad (r = 1, \ldots, s)$$

und, wenn man diese Reihe identischer Kongruenzen miteinander multipliziert und wieder passend ordnet, auch:

$$\sum_{i=1}^{h} F_i \mu_i'' + P^{a_1}_{k+1,1} \ldots P^{a_s}_{k+1,s} \nu \equiv 1 \ \left(\text{mod. } (P^{(k)})\right).$$

Aus der Darstellung der Resolventenform ergibt sich aber die weitere identische Relation

$$P^{a_1}_{k+1,1} \ldots P^{a_s}_{k+1,s} \equiv \sum_{i=1}^{h} \lambda_i' F_i \ \left(\text{mod } (P^{(k)})\right)$$

und demnach endlich die gesuchte Lösung in der identischen Kongruenz:

$$\sum_{i=1}^{h} F_i (\mu_i' + \lambda_i' \nu) \equiv 1 \ \left(\text{mod. } (P^{(k)})\right).$$

Damit ist aber die als „zweites Fundamentalproblem" bezeichnete Aufgabe in einer endlichen Anzahl von Schritten vollständig erledigt, da sie schließlich auf die Bestimmung einer Lösung von Kongruenzen der Gestalt

$$\sum_{i=1}^{h} F_i X_i \equiv 1 \ \left(\text{mod. } (P^{(m-1)})\right)$$

zurückgeführt wird; für diese Kongruenz haben wir aber nicht nur eine, sondern auch die allgemeine Lösung in § 7 gefunden.

Für unsre Zwecke genügt übrigens die Bemerkung, daß der größte gemeinschaftliche Teiler von $F_1, \ldots, F_h$ in ganz elementarer Weise (nach dem Euklidischen Verfahren) bestimmt werden kann, und, wenn dieser sich $\sim 1 \ \left(\text{mod. } (P^{(m-1)})\right)$ ergibt, dasselbe Verfahren auch eine Relation

$$\sum_{i=1}^{h} F_i \lambda_i \equiv 1 \ (\text{mod. } P^{(m-1)})$$

ergibt.

Gattungsbereiche mod. $(P^{(k)})$.

§ 9. Ist $F(x_l, x_{l-1}, \ldots, x_1)$ eine rationale und ganze Form, die x_l wirklich enthält, und $l > k$, so gibt die Kongruenz

$$F(x_l, x_{l-1}, \ldots, x_1) \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

wörtlich zu denselben Betrachtungen Anlaß, die für den Fall $k = -1$ in Kap. IV durchgeführt wurden.

Ist insbesondere $F(x_l, x_{l-1}, \ldots)$ irreduzibel mod. $(P^{(k)})$ und vom Grade n in x_l, so gelangt man genau so, wie in Kap. IV. § 6, in dieser Weise zu dem pseudoorthoiden Bereiche

$$\frac{G_0 + G_1\alpha + \cdots + G_{n-1}\alpha^{n-1}}{H} \ \left(\text{mod. } (P^{(k)})\right),$$

wo $G_0, \ldots, G_{n-1}, H$ rationale und ganze Formen von $x_1, \ldots, x_{l-1}$ „mod. $(P^{(k)})$" sind und H nicht $\equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$. Zwei Größen dieses Bereichs

$$\frac{G_0 + G_1\alpha + \cdots + G_{n-1}\alpha^{n-1}}{H} \quad \text{und} \quad \frac{G_0' + G_1'\alpha + \cdots + G_{n-1}'\alpha^{n-1}}{H'}$$

sind dann und nur dann „gleich", d. h. kongruent mod. $(P^{(k)})$, wenn

$$H' G_i \equiv H G_i' \quad \left(\text{mod. } (P^{(k)})\right) \quad (i = 0, 1, \ldots, n-1)$$

ist. Die Addition und Multiplikation dieser Größen geschieht nach den gewöhnlichen Regeln der Algebra, wenn man noch die Anweisung hinzufügt, daß die n^{te} und höhere Potenzen von α mittels der identischen Relation

$$F(\alpha, x_{l-1}, \ldots, x_1) \equiv 0 \quad \left(\text{mod. } (P^{(k)})\right)$$

aus dem Resultate zu entfernen sind. Diese Anweisung besagt, daß in dem neuen Bereiche α Wurzel der Kongruenz $F \equiv 0$ ist.

Der neue Bereich soll kurz als „durch Adjunktion einer Wurzel der Kongruenz $F \equiv 0$ $\left(\text{mod. } (P^{(k)})\right)$ aus $(l-1)$ $\left(\text{mod. } (P^{(k)})\right)$ entstanden" charakterisiert und mit

$$((l-1), \alpha) \quad \left(\text{mod. } (P^{(k)})\right)$$

bezeichnet werden, wo wir für den orthoiden Bereich

$$([1], x_1, \ldots, x_{l-1})$$

die abgekürzte Bezeichnung $(l-1)$ eingeführt haben; die Größen des Bereichs sind „mod. $(P^{(k)})$ zu betrachtende (absolute) algebraische Größen".

Der Bereich $((l-1), \alpha)$ $\left(\text{mod. } (P^{(k)})\right)$ ist in dem in Kap. IV. § 7 erörterten Sinne der „kleinste" pseudoorthoide Bereich, in dem die Kongruenz $F(z) \equiv 0$ $\left(\text{mod. } (P^{(k)})\right)$ eine Wurzel besitzt.

In vollkommener Analogie mit den Entwicklungen in Kap. IV. § 10 können wir auch den „Galoisschen Bereich mod. $P^{(k)}$" konstruieren, in dem die Kongruenz $F(z) \equiv 0$ genau ebensoviel Wurzeln besitzt, als ihr Grad in x_l Einheiten zählt. Ebenso erhält man hieraus weiter, (wie in Kap. IV. § 14. 15) die dem Bereiche $(l-1)$ entstammenden Gattungsbereiche mod. $(P^{(k)})$, dessen konjugierte Bereiche und die hierauf bezüglichen einzelnen Sätze, die dort aufgezählt wurden.

Die Faktorenzerlegung der einem Gattungsbereiche $((l-1), \alpha)$ $(\text{mod. } (P^{(k)}))$ entstammenden Formen befolgt wieder dieselben Gesetze und Regeln, die für den einfachsten Fall, $k = -1$, in Kap. IV. § 16 auseinandergesetzt wurden. Endlich ersieht man — in voller Analogie mit Kap. IV. § 19 —, daß die dem Bereiche $((l-1), \alpha)$ $(\text{mod. } (P^{(k)}))$ entstammenden Gattungsbereiche wieder mit dem Bereiche $(l-1)$ $(\text{mod. } (P^{(k)}))$ entstammenden Gattungsbereichen $(\text{mod. } (P^{(k)}))$ identisch sind.

Ist $l = k+1$, und $k > -1$, so sind in dem Bereiche $((k), \alpha)$ $(\text{mod. } (P^{(k)}))$ nur eine endliche Anzahl von Größen vorhanden; die so definierten algebraischen Größen sind für $k=0$ nichts anderes als die von Galois in die Zahlentheorie eingeführten imaginären Größen. Dieser Fall, in dem die Aussage einzelner Sätze modifiziert werden muß, wird in den weiteren Entwicklungen dieses Buches nicht zur Anwendung gelangen; im folgenden soll daher immer $l \geqq k+2$ vorausgesetzt werden.

Es seien

$$\Phi_j(z_1, z_2, \ldots, z_j) \qquad (j = 1, \ldots, r)$$

wirkliche Formen von $z_1, \ldots, z_j$, deren Koeffizienten dem Bereiche $[[1], x_1, \ldots, x_s]$ $(\text{mod. } (P^{(k)}))$ entstammen, und es soll noch insbesondere der Koeffizient der höchsten Potenz von z_j in Φ_j diesem Bereiche angehören; und es sei $s \geqq k+1$. Es sei ferner Φ_1 irreduzibel mod. $(P^{(k)})$; der durch Adjunktion einer Wurzel von $\Phi_1 \equiv 0$ entstandene Gattungsbereich sei $((s), \alpha_1)$ $(\text{mod. } (P^{(k)}))$ und $\Phi_2(\alpha_1, z_2)$ wieder irreduzibel mod. $(P^{(k)})$ in $((s), \alpha_1)$; durch Adjunktion einer Wurzel der Kongruenz $\Phi_2(\alpha_1, z_2) \equiv 0$ entstehe der Gattungsbereich $((s), \alpha_1, \alpha_2)$ $(\text{mod. } (P^{(k)}))$ u. s. f., bis endlich $\Phi_r(\alpha_1, \ldots, \alpha_{r-1}, z_r)$ irreduzibel in $((s), \alpha_1, \ldots, \alpha_{r-1})$ $(\text{mod. } (P^{(k)}))$ vorauszusetzen und durch Adjunktion einer Wurzel der Kongruenz

$$\Phi_r(\alpha_1, \ldots, \alpha_{r-1}, z_r) \equiv 0$$

der Bereich $((s), \alpha_1, \ldots, \alpha_r)$ $(\text{mod. } (P^{(k)}))$ entsteht.

Ist nun Ψ irgend eine Form von $z_1, \ldots, z_r$ mit Koeffizienten aus $[[1], x_1, \ldots, x_s]$ $\left(\text{mod. } (P^{(k)})\right)$, so wird man nach dem gewöhnlichen Divisionsverfahren eine Relation

$$G\Psi \equiv \Sigma A_j \Phi_j + R \left(\text{mod. } (P^{(k)})\right)$$

finden, wo G eine rationale und ganze, mod. $(P^{(k)})$ von 0 verschiedene Form der x ist, während R eine Form der z wird, die in z_j höchstens vom Grade $n_j - 1$ ist, wenn Φ_j in z_j vom Grade n_j ist. Nach der Definition der Größen α ist demnach

$$R(\alpha_1, \ldots, \alpha_r) \left(\text{mod. } (P^{(k)})\right)$$

dann und nur dann Null, wenn die Form $R(z_1, \ldots, z_r)$ $\left(\text{mod. } (P^{(k)})\right)$ verschwindet, und dies findet wieder dann und nur dann statt, wenn

$$\Psi(\alpha_1, \ldots, \alpha_r) \equiv 0 \left(\text{mod. } (P^{(k)})\right).$$

In diesem Falle ist also auch

$$G\Psi \equiv 0 \left(\text{mod. } \Phi_1, \ldots, \Phi_r, (P^{(k)})\right).$$

Verbindet man dieses Resultat mit dem Satze des § 7 in Kapitel VII, so ergibt sich endlich:

I. Ist Ψ irgend eine Form, für die $\Psi(\alpha_1, \ldots, \alpha_r) \equiv 0$ $\left(\text{mod. } (P^{(k)})\right)$, so gibt es eine bestimmte rationale und ganze Form K der x, die mod. $(P^{(k)})$ von 0 verschieden, und für welche

$$K\Psi \equiv 0 \left(\text{mod. } \Phi_1, \ldots, \Phi_r, (P^{(k)})\right)$$

wird. Insbesondere ersieht man — genau wie an der citierten Stelle —, daß die Bestimmung der Form K in einer endlichen Anzahl von Schritten erledigt ist, wenn die allgemeine Lösung der homogenen linearen Kongruenz

$$\Sigma F_i X_i \equiv 0 \ (\text{mod. } P^{(k)})$$

im Bereiche $[[1], z_1, \ldots, z_r, x_1, \ldots, x_s]$ bekannt ist.

Man bemerke dabei noch folgendes: Ist φ_j der Koeffizient der höchsten Potenz von z_j in Φ_j, so enthält K

jedenfalls nur diejenigen Unbestimmten x, die in $\varphi_1, \ldots, \varphi_r$ wirklich auftreten.

Ist aber zweitens $\Psi(\alpha_1, \ldots, \alpha_r)$ nicht $\equiv 0 \left(\text{mod. } (P^{(k)})\right)$, also auch $R(\alpha_1, \ldots, \alpha_r)$ von 0 verschieden, so kann man eine zweite Größe des Bereichs $((s), \alpha_1, \ldots, \alpha_r)$ in derselben Gestalt wie R so bestimmen, daß

$$S(\alpha_1, \ldots, \alpha_r) R(\alpha_1, \ldots, \alpha_r) \equiv 1 \left(\text{mod. } (P^{(k)})\right),$$

und demnach

$$GS(\alpha_1, \ldots, \alpha_r) \Psi(\alpha_1, \ldots, \alpha_r) - 1 \equiv 0 \left(\text{mod. } (P^{(k)})\right)$$

wird. Dabei ist der Nenner in S eine mod. $(P^{(k)})$ von 0 verschiedene rationale und ganze Form von $x_1, \ldots, x_s$. Multipliziert man mit diesem Nenner und der früher bestimmten Form K, so erhält man endlich für diesen zweiten Fall folgenden Satz:

II. Ist $\Psi(\alpha_1, \ldots, \alpha_r)$ nicht $\equiv 0 \left(\text{mod. } (P^{(k)})\right)$, so gibt es eine zweite rationale und ganze Form X der x und z und eine rationale und ganze Form H der x, die beide mod. $(P^{(k)})$ von 0 verschieden sind und die Eigenschaft besitzen, daß

$$\Psi X \equiv H \left(\text{mod. } \Phi_1, \ldots, \Phi_r, (P^{(k)})\right)$$

wird. Die Bestimmung von Ψ und H ist jedenfalls wieder mit dem früher erwähnten diophantischen Probleme zugleich erledigt.

Arithmetische Theorie der homogenen linearen diophantischen Gleichungen. Die Prinzipien der Reduktion.

§ 10. Wir sind nun im Besitze der wesentlichen Hilfsmittel, um die Auflösung der Gleichung $\Sigma F_j X_j = 0$ im Bereiche $[[1], x_1, \ldots, x_m]$ vollständig zu erledigen. Dies geschieht durch eine allgemeine Methode, nach welcher das Problem in $[[1], x_1, \ldots, x_m]$ auf das Problem in $[[1], x_1, \ldots, x_{m-1}]$ zurückgeführt wird. Daß diese Reduktion bei der Allgemeinheit der

Aufgabe nicht sonderlich einfach sein kann, ist wohl selbstverständlich. Dabei nehmen die Fälle $m = 1$ und 2, die in gewisser Beziehung als elementar betrachtet werden können, eine Sonderstellung ein, auf die an der geeigneten Stelle noch hingewiesen werden wird.

Das Problem soll von vornherein als das der Lösung der Kongruenz

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

gefaßt werden, die nur formell allgemeiner als die Gleichung $\Sigma F_j X_j = 0$ ist und für $k = -1$ in diese übergeht.

Die Fälle $k = m$ und $k = m - 1$ erledigen sich in völlig elementarer Weise.

Für $k = m$ können zuerst alle Koeffizienten $\equiv 0 \ \left(\text{mod. } (P^{(m)})\right)$ sein; und die Formen X_j unterliegen dann überhaupt keiner weiteren Beschränkung. — Ist dies nicht der Fall, also z. B. F_1 nicht $\equiv 0 \ \left(\text{mod. } (P^{(m)})\right)$, so gibt es eine Form G, für die

$$G F_1 \equiv 1 \ \left(\text{mod. } (P^{(m)})\right),$$

und die Kongruenz geht durch Multiplikation mit G in

$$X_1 + \sum_{j=2}^{h} G F_j X_j \equiv 0 \ \left(\text{mod. } (P^{(m)})\right)$$

über, deren Lösung unmittelbar hingeschrieben werden kann.

Für den Fall $k = m - 1$ muß wieder nur der Fall betrachtet werden, in dem nicht sämtliche Koeffizienten $\equiv 0$ mod. $(P^{(m-1)})$ sind. (Für $m = 0$, wenn nicht sämtliche Koeffizienten verschwinden). Man kann nun weiter den größten gemeinschaftlichen Teiler mod. $(P^{(m-1)})$ der F entfernen; ist dann einer der Koeffizienten $\equiv \pm 1$, so ist die allgemeine Lösung der Kongruenz evident. Im entgegengesetzten Falle sei F_1 in irreduzible Faktoren $\left(\text{mod. } (P^{(m-1)})\right)$ zerlegt:

$$F_1 \equiv \pi_1 \pi_2 \ldots \ \left(\text{mod. } (P^{(m-1)})\right).$$

Dann wird eine der Formen F, z. B. F_h nicht teilbar mod. $(P^{(m-1)})$ durch π_1 sein; andrerseits muß dann

$$\sum_{j=2}^{h} F_j X_j \equiv 0 \left(\text{mod. } \pi_1, (P^{(m-1)})\right)$$

sein. Das hier zur Anwendung gelangende Modulsystem ist, wie unmittelbar ersichtlich, ein P-System $m + 1^{\text{ter}}$ Stufe, und nach ihm F_h nicht $\equiv 0$. Es gibt daher eine leicht zu bestimmende Form G, für die

$$GF_h \equiv -1 \left(\text{mod. } \pi_1, (P^{(m-1)})\right)$$

ist, und es muß demnach

$$X_h \equiv \sum_{j=2}^{h-1} F_j G X_j \text{ (mod. } \pi_1, P^{(m-1)})$$

oder auch

$$X_h \equiv \sum_{j=2}^{h-1} F_j G X_j + \pi_1 Y \left(\text{mod. } (P^{(m-1)})\right)$$

sein. Die gegebene Kongruenz geht daher in

$$F_1 X_1 + \sum_{j=2}^{h-1} F_j (F_h G + 1) X_j + F_h \pi_1 Y \equiv 0 \left(\text{mod. } (P^{(m-1)})\right)$$

über. Hier sind sämtliche Koeffizienten durch π_1 teilbar; dieser Teiler darf entfernt werden, und unsre Kongruenz ist mit

$$\frac{F_1}{\pi_1} X_1 + \sum_{j=2}^{h-1} F_j \frac{F_h G + 1}{\pi_1} X_j + F_h Y \equiv 0 \text{ (mod. } P^{(m-1)})$$

zugleich gelöst. Aber der Koeffizient von X_1 ist statt F_1 jetzt $\frac{F_1}{\pi_1}$, und man gelangt daher in einer endlichen Anzahl von Schritten zu einer Kongruenz, in welcher der Koeffizient von X_1 gleich ± 1 ist, und damit zur allgemeinen Lösung unsrer Aufgabe.

Für $m = 0$ ist dies nichts anderes als die elementare Lösung der diophantischen Gleichung $\Sigma a_j x_j = 0$ in [1].

Unser Problem ist also allgemein gelöst, wenn wir seine Reduktion von m auf $m - 1$ bewerkstelligen, und dabei kann die Auflösung jedes linearen diophantischen Systems in $[[1], x_1, \ldots, x_{m-1}]$ als gegeben angesehn werden,

da das zweite Fundamentalproblem, Bestimmung einer Lösung von $\Sigma F_j X_j = 1$, falls eine solche existiert, schon früher vollständig erledigt wurde.

§ 11. Im Bereiche $[[1], x_1, \ldots, x_m]$ ist die Theorie der Kongruenz

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \pmod{P^{(k)}}$$

erledigt, wenn $k = m$ oder $k = m - 1$ ist. Dasselbe ist aber auch dann der Fall, wenn $k < m - 1$, und die Koeffizienten eine der Unbestimmten $x_{k+1}, \ldots, x_m$, z. B. x_m nicht enthalten.

Ordnen wir in diesem Falle die Unbekannten X_j nach Potenzen von x_m und setzen demnach

$$X_j = X_{j0} + X_{j1} x_m + \cdots + X_{jr} x_m^r + \cdots,$$

so muß auch

$$\Sigma F_j X_{jr} \equiv 0 \left(\mathrm{mod.}\ (P^{(k)})\right)$$

sein, und hieraus ergibt sich, da wir es nun mit einem Probleme in $[[1], x_1, \ldots, x_{m-1}]$ zu tun haben,

$$X_{jr} \equiv \sum_{(s)} G_{js} U_{rs} \left(\mathrm{mod.}\ (P^{(k)})\right),$$

wo die G_{js} gegebene, von r unabhängige, die U_{rs} beliebige rationale und ganze Formen von $x_1, \ldots, x_{m-1}$ sind. Dies ergibt für unsern Fall die allgemeine Lösung

$$X_j \equiv \sum_{(s)} G_{js} V_s \left(\mathrm{mod.}\ (P^{(k)})\right),$$

wo die

$$V_s = \sum_{(r)} U_{rs} x_m^r,$$

also beliebige Formen von $x_1, \ldots, x_m$ sind.

Das spezielle Problem, alle Formen zu bestimmen, die der Kongruenz

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \mod (P^{(k)})$$

genügen und dabei in x_m den Grad n nicht übersteigen, ist nun gleichfalls als gelöst zu betrachten. Ordnet man nämlich F_j und auch die Unbekannten X_j nach Potenzen von x_m, so muß in $\Sigma F_j X_j$ der Koeffizient jeder Potenz von x_m jetzt $\equiv 0 \left(\mathrm{mod.}\,(P^{(k)})\right)$ sein, und dies ergibt ein System von homogenen linearen diophantischen Gleichungen in $[[1], x_1, \ldots, x_{m-1}]$, in denen die Formen X_{jr} aus

$$X_j = \sum_{r=0}^{n} X_{jr} x_m^r$$

die Unbekannten sind.

Schließlich sei noch die Gleichung

$$P_{m+1} X_{m+1} + P_m X_m + \cdots + P_1 X_1 + p_0 X_0 = 0,$$

in der die Koeffizienten ein P-System $m+1^{\text{ter}}$ Stufe bilden, erwähnt, deren allgemeine Lösung sofort hingeschrieben werden kann.

Da $P_{m+1} X_{m+1} \equiv 0 \left(\mathrm{mod.}\,(P^{(m)})\right)$ und P_{m+1} nicht $\equiv 0 \left(\mathrm{mod.}\,(P^{(m)})\right)$ ist, muß

$$X_{m+1} \equiv P_m U_m + \cdots + P_1 U_1 + p_0 U_0 \qquad \text{(a)}$$

sein; damit geht aber die Gleichung in

$$P_m (X_m + P_{m+1} U_m) + \cdots + P_1 (X_1 + P_{m+1} U_1) + \\ + p_0 (X_0 + P_{m+1} U_0) = 0$$

über, aus der sich wieder

$$X_m + P_{m+1} U_m = P_{m-1} U_{m-1}^{(1)} + \cdots + P_1 U_1^{(1)} + p_0 U_0^{(1)} \qquad \text{(b)}$$

ergibt. Daraus folgt wieder

$$P_{m-1} (X_{m-1} + P_{m+1} U_{m-1} + P_m U_{m-1}^{(1)}) + \cdots + \\ + p_0 (X_0 + P_{m+1} U_0 + P_m U_0^{(1)}) = 0$$

und

$$X_{m-1} + P_{m+1} U_{m-1} + P_m U_{m-1}^{(1)} = P_{m-2} U_{m-2}^{(2)} + \cdots + p_0 U_0^{(2)} \qquad \text{(c)}$$

u. s. f. Daß diese notwendige Gestalt der Unbekannten immer auch hinreicht, um eine Lösung der vorgelegten Gleichung zu liefern, ist unmittelbar einzusehn.

Für die Darlegung der allgemeinen Methode ist noch die folgende Bemerkung von Wichtigkeit. Die Kongruenz

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

kann, wenn wir die links stehenden Glieder irgendwie in zwei Abteilungen sondern, auch

$$\sum_{j'=1}^{h'} F'_{j'} X'_{j'} + \sum_{j''=1}^{h''} F''_{j''} X''_{j''} \equiv 0 \ (\text{mod. } P^{(k)}), \quad (h' + h'' = h) \tag{1}$$

geschrieben werden, und ihre allgemeine Lösung liefert auch die allgemeine Lösung der Kongruenz

$$\sum_{j'=1}^{h'} F'_{j'} X'_{j'} \equiv 0 \ \left(\text{mod. } F''_1, \ldots, F''_{h''}, (P^{(k)})\right), \tag{2}$$

da hierbei nur von den Werten der Unbekannten X'' abgesehn wird.

Das Umgekehrte findet nur in speziellen Fällen statt. Jedenfalls müssen die Unbekannten X' in (1) die aus (2) resultierende Gestalt

$$X'_{j'} \equiv \sum_{(s)} G_{j's} U_s \ (\text{mod. } F''_1, \ldots, F''_{h''}, P^{(k)}) \tag{3}$$

haben, und da diese bei beliebiger Wahl der Formen U_s eine Lösung von (2) ergeben, muß weiter, bei Einsetzung der Werte aus (3) in

$$\sum_{j'=1}^{h'} F'_{j'} X'_{j'} \equiv \sum_{(s)} H_s U_s,$$

jede Form $H_s \equiv 0 \ \left(\text{mod. } F'', \ldots, F''_{h''}, (P^{(k)})\right)$ sein.

Kennt man eine Darstellung

$$H_s \equiv \sum_{j''=1}^{h''} A_{j''s} F''_{j''} \ \left(\text{mod. } (P^{(k)})\right), \tag{4}$$

so geht nach Auflösung von (2) die Kongruenz (1) in

$$\sum_{j''=1}^{h''} F''_{j''} (X''_{j''} + A_{j''1} U_1 + A_{j''2} U_2 + \cdots) \equiv 0 \ \left(\text{mod. } (P^{(k)})\right) \tag{5}$$

über.

Die Kongruenz (1) kann daher insbesondere in zwei speziellen Fällen vollständig durch (2) ersetzt werden, erstens, wenn $h'' = 1$, und zweitens, wenn die Formen F'' eine der Unbestimmten $x_{k+2}, \ldots, x_m$, z. B. x_m nicht enthalten.

Im ersten Falle sind die in (4) und (5) gestellten Aufgaben unmittelbar gelöst; im zweiten Falle haben wir es mit linearen diophantischen Problemen im Bereiche $[[1], x_1, \ldots, x_{m-1}]$ zu tun.

§ 12. Die allgemeine Lösung der Kongruenz

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \left(\text{mod. } (P^{(k)})\right)$$

wurde in den bisherigen Entwicklungen für $k = m$ und $m - 1$ gegeben; sie wird also für alle Fälle bewerkstelligt sein, wenn wir das Problem auf die Lösung einer ebensolchen Kongruenz mod. $(P^{(k+1)})$ zurückführen. Dies soll nun geschehn.

In einfachster Weise gelingt die Lösung, wenn ein Koeffizient nur die Unbestimmten $x_1, \ldots, x_k, x_{k+1}$ enthält. Die Kongruenz kann dann in der Gestalt

$$\Phi^{(k+1)} Y + G_1 Z_1 + \cdots \equiv 0 \left(\text{mod. } (P^{(k)})\right)$$

geschrieben werden, wo $\Phi^{(k+1)}$ eine mod. $(P^{(k)})$ von 0 verschiedene rationale und ganze Form von $x_1, \ldots, x_{k+1}$ ist.

Ist nun $\Phi^{(k+1)} \simeq 1 \left(\text{mod. } (P^{(k)})\right)$, also

$$\Psi \Phi^{(k+1)} \equiv -1 \left(\text{mod. } (P^{(k)})\right),$$

so ergibt sich unmittelbar

$$Y \equiv \Psi G_1 Z_1 + \cdots \left(\text{mod. } (P^{(k)})\right).$$

Für den Fall, wo $\Phi^{(k+1)}$ nicht $\simeq 1 \left(\text{mod. } (P^{(k)})\right)$ ist, kann man $\Phi^{(k+1)}$ in mod. $(P^{(k)})$ irreduzible Faktoren zerlegen:

$$\Phi^{(k+1)} \equiv \pi_1 \pi_2 \ldots \left(\text{mod. } (P^{(k)})\right)$$

und die Kongruenz in der Gestalt

$$\pi_1 (\pi_2 \cdots Y) + G_1 Z_1 + \cdots \equiv 0 \left(\text{mod. } (P^{(k)})\right)$$

schreiben. Es muß also

$$G_1 Z_1 + \cdots \equiv 0 \left(\text{mod. } \pi_1, (P^{(k)})\right)$$

sein. Das hier auftretende Modulsystem ist aber geradezu ein P-System $k+1^{\text{ter}}$ Stufe; die allgemeine Lösung dieser Kongruenz kann also als bekannt vorausgesetzt werden. Sie ergibt

$$Z_i \equiv \sum_{(s)} H_{is} U_s + \pi_1 Y_i \left(\text{mod. } (P^{(k)})\right)$$

und

$$\pi_2 \cdots Y \equiv \sum_{(s)} K_s U_s + \sum_{(l)} G_i Y_i \left(\text{mod. } (P^{(k)})\right).$$

Mit der Lösung dieser letzten Kongruenz ergibt sich die spezielle Gestalt der U und Y und damit auch die der Z. In der nun zu lösenden Kongruenz ist aber der Koeffizient von Y nur mehr $\frac{\Phi^{(k+1)}}{\pi_1}$; man gelangt also in einer endlichen Anzahl von Schritten zum Koeffizienten $\frac{\Phi^{(k+1)}}{\pi_1 \pi_2 \cdots} \equiv 1 \left(\text{mod. } (P^{(k)})\right)$, d. h. zur definitiven Lösung der vorgelegten Aufgabe.

§ 13. Allgemein sei in der vorgelegten Kongruenz ein Koeffizient vorhanden, der außer $x_1, \ldots, x_k$ nur mehr die Unbestimmten $x_{k+1}, \ldots, x_l$ enthält, und $l > k+1$. Mit der Reduktion dieses Falles auf denjenigen, wo ein Koeffizient außer $x_1, \ldots, x_k$ nur mehr $x_{k+1}, \ldots, x_{l-1}$ enthält, gelangt man in einer endlichen Anzahl von Schritten zu einer Kongruenz, deren Lösung schon bekannt ist, d. h. zur vollständigen Lösung des vorgelegten Problems.

Dabei genügt es, jenen Koeffizienten $\Phi^{(l)}(x_1, \ldots, x_l)$ als mod. $(P^{(k)})$ irreduzibel anzunehmen. Der Fall, wo $\Phi^{(l)}$ das Produkt mehrerer mod. $(P^{(k)})$ irreduzibeln Faktoren ist, erledigt sich dann wörtlich nach der am Ende des vorhergehenden Paragraphen angewandten Methode.

Es kann nun weiter angenommen werden, daß in der vorgelegten Kongruenz, die wir

$$\Phi^{(l)} Y + G_1 Z_1 + G_2 Z_2 + \cdots \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

schreiben, kein Koeffizient G durch $\Phi^{(l)}$ teilbar mod. $(P^{(k)})$ ist. Wäre z. B.

$$G_1 \equiv \Phi^{(l)} H_1 \ \left(\text{mod. } (P^{(k)})\right),$$

so kann die Kongruenz auch

$$\Phi^{(l)} (Y + H_1 Z_1) + G_2 Z_2 + \cdots \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

geschrieben werden und ist, wenn man

$$Y + H_1 Z_1 = Y_1$$

setzt, mit der Kongruenz

$$\Phi^{(l)} Y_1 + G_2 Z_2 + \cdots \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

zugleich allgemein gelöst. In dieser aber ist das Glied mit dem durch $\Phi^{(l)}$ teilbaren Koeffizienten G_1 ganz herausgefallen.

Die in Aussicht genommene Reduktion kann unmittelbar ausgeführt werden, wenn in der Kongruenz noch ein zweiter Koeffizient vorhanden ist, der nur die Unbestimmten $x_1, \ldots, x_k, \ldots, x_l$ enthält. Die Kongruenz kann dann auch

$$\Phi^{(l)} Y_1 + \Psi^{(l)} Y_2 + G_1 Z_1 + \cdots \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

oder (nach der Schlußbemerkung des § 11)

$$\Psi^{(l)} Y_2 + G_1 Z_1 + \cdots \equiv 0 \ \left(\text{mod. } \Phi^{(l)}, (P^{(k)})\right)$$

geschrieben werden.

Da $\Phi^{(l)}$ irreduzibel mod. $(P^{(k)})$ und $\Psi^{(l)}$ durch $\Phi^{(l)}$ nicht teilbar mod. $(P^{(k)})$ ist, wird die Resultante von $\Psi^{(l)}$ und $\Phi^{(l)}$ nach x_l:

$$\varrho = \mu \Phi^{(l)} + \nu \Psi^{(l)}$$

nicht $\equiv 0$ (mod. $P^{(k)}$) sein und selbstverständlich x_l nicht enthalten. Da ferner ν nicht durch $\Phi^{(l)}$ teilbar mod. $(P^{(k)})$, und $\Phi^{(l)}$ irreduzibel ist, kann jene Kongruenz auch

$$\nu (\Psi^{(l)} Y_2 + G_1 Z_1 + \cdots) \equiv 0 \ \left(\text{mod. } \Phi^{(l)}, (P^{(k)})\right)$$

oder endlich auch

$$\varrho Y_2 + \Phi^{(l)} Y_3 + \nu G_1 Z_1 + \cdots \equiv 0 \pmod{P^{(k)}}$$

geschrieben werden, wo der Koeffizient ϱ nur mehr die Unbestimmten $x_1, \ldots, x_{l-1}$ enthält. Für den Fall $l = 1$ wird ϱ eine rationale ganze, von 0 verschiedene Zahl.

Damit ist aber das Problem der homogenen linearen diophantischen Gleichung im Bereiche $[[1], x_1]$ vollständig erledigt.

In diesem sind die Koeffizienten der Unbekannten rationale und ganze Formen einer Unbestimmten. Die soeben vorgetragene Reduktion führt die Lösung der Gleichung auf eine solche zurück, in welcher einer der Koeffizienten eine rationale und ganze Zahl ist. (Dabei ist von dem trivialen Falle $FX = 0$, aus dem $X = 0$ folgt, abgesehn.)

Nach § 12 verlangt das Problem dann nur mehr die Auflösung von Kongruenzen

$$\Sigma G_i Z_i \equiv 0 \pmod{p}$$

im Bereiche $[[1], x_1]$, wo p eine natürliche Primzahl bedeutet. Hier ist $k = 0$, $m = 1$, und die Auflösung demnach schon in § 10 vollständig gegeben.

§ 14. Der weitere Gang der Reduktion ist folgender. Wir haben es jetzt mit einer Kongruenz

$$\Sigma F_j X_j \equiv 0 \left(\text{mod. } \Phi^{(l)}, (P^{(k)})\right) \qquad \text{(I)}$$

zu tun, wo $\Phi^{(l)}$ eine mod. $(P^{(k)})$ irreduzible rationale und ganze Form von $x_1, \ldots, x_l$, $l > k + 1$, und endlich kein Koeffizient F_j teilbar mod. $(P^{(k)})$ durch $\Phi^{(l)}$ ist.

Dabei kann aber auch $l < m$ angenommen werden. Wenn $l = m$, und die Unbestimmte x_m in allen Koeffizienten F_j wirklich vorkommt, ist die Reduktion von $l = m$ auf $l = m - 1$ eben vorher ausgeführt worden. Ist aber z. B. F_1 eine Form, die x_m nicht enthält, so ist diese, resp. einer ihrer irreduzibeln Teiler an die Stelle von $\Phi^{(l)}$ zu setzen, und dann ist in der Tat wieder $l < m$.

Der Fall, wo die Unbestimmte x_m in keinem der Koeffizienten F vorkommt, ist nach § 11 als erledigt zu betrachten.

Enthält ein F die Unbestimmte x_m, während alle andern Koeffizienten $\equiv 0 \pmod{\Phi^{(l)}, P^{(k)}}$ sind, so haben wir es mit der Kongruenz

$$FX + \Phi^{(l)} Y \equiv 0 \left(\mathrm{mod.}\ (P^{(k)})\right)$$

zu tun, die wir in die Reihe der später gesondert zu behandelnden singulären Fälle verweisen.

Ist ein F vorhanden, das x_m nicht enthält, so kann die Kongruenz auch

$$\Sigma G_j Y_j \equiv 0 \left(\mathrm{mod.}\ \Psi, \Phi^{(l)}, (P^{(k)})\right) \qquad \text{(II)}$$

geschrieben werden, wo Ψ eine rationale und ganze Form von $x_1, \ldots, x_{m-1}$ bedeutet, die mod. $(P^{(k)})$ nicht durch $\Phi^{(l)}$ teilbar ist.

Endlich mögen alle F die Unbestimmte x_m enthalten, und es sei z. B. F_1 vom niedrigsten, ν^{ten} Grade in x_m. Nach dem gewöhnlichen Divisionsverfahren wird man dann Relationen

$$\Psi F_j \equiv Q_j F_1 + R_j \left(\mathrm{mod.}\ (P^{(k)})\right)$$

finden, wo R_j eine Form vom höchstens $\nu - 1^{\text{ten}}$ Grade in x_m ist, und Ψ eine Potenz des Koeffizienten von x_m^ν in F_1, also auch mod. $\left(\Phi^{(l)}, (P^{(k)})\right)$ von 0 verschieden ist. Da aber $\left(\Phi^{(l)}, (P^{(k)})\right)$ ein Primsystem ist, kann die vorgelegte Kongruenz auch

$$F_1(\Psi X_1 + Q_2 X_2 + \cdots) + R_2 X_2 + \cdots \equiv 0 \left(\mathrm{mod.}\ \Phi^{(l)}, (P^{(k)})\right)$$

geschrieben werden, in der, wenn man $\Psi X_1 + Q X_2 + \cdots$ als neue Unbekannte auffaßt, nun der Koeffizient F_1 vom höchsten Grade in x_m ist. Die Wiederholung dieser Reduktion führt aber in einer endlichen Anzahl von Schritten entweder zu dem schon früher erwähnten singulären Falle, oder aber zu einer Kongruenz von der Gestalt (II), und die inzwischen aufzulösenden Kongruenzen

$$\Psi X_1 + Q X_2 + \cdots \equiv \Sigma H_s U_s \left(\mathrm{mod.}\ \Phi^{(l)}, (P^{(k)})\right)$$

haben dieselbe Gestalt, d. h. die allgemeine Lösung der Kongruenz (I) ist — mit Ausnahme des singulären Falls — auf die allgemeine Lösung der Kongruenz (II) zurückgeführt.

Damit ist aber das Problem der homogenen linearen diophantischen Gleichung im Bereiche $[[1], x_1, x_2]$ vollständig erledigt.

In diesem Falle ist nach den Erörterungen zu Beginn dieses Paragraphen $l > 0$ und $l < 2$, also $l = 1$. Es sind also in (II) sowohl Ψ wie $\Phi^{(l)}$ Formen der einen Unbestimmten x_1. Nach § 13 reduziert sich das Problem dann auf eine homogene lineare Kongruenz (mod. p), die nach den in § 12 dargelegten Methoden vollständig gelöst ist. Enthalten alle Koeffizienten die beiden Unbestimmten x_1, x_2, so kommt man nach der soeben dargelegten Methode entweder auf den singulären Fall, oder aber auf eine Kongruenz von der Gestalt (II), wo $l < 2$ ist, deren vollständige Lösung wieder nach § 12 bekannt ist. Der singuläre Fall ist nun entweder

$$FX + \Phi^{(l)} Y = 0,$$

wo man schon F und $\Phi^{(l)}$ ohne gemeinschaftlichen Teiler voraussetzen kann, und also die allgemeine Lösung

$$X = \Phi^{(l)} U, \quad Y = -FU$$

unmittelbar hinschreiben kann. Oder aber

$$FX + \Phi^{(l)} Y \equiv 0 \pmod{p}.$$

Auch diese Kongruenz ist unmittelbar gelöst. Die Lösung ist evident, wenn F oder $\Phi^{(l)} \equiv 0 \pmod{p}$. Ist keine dieser Formen $\equiv 0 \pmod{p}$, so kann man wieder den größten gemeinschaftlichen Teiler (mod. p) von F und $\Psi^{(l)}$ entfernen und erhält dann die allgemeine Lösung

$$X \equiv \bar{\Phi}^{(l)} U, \quad Y \equiv -\bar{F} U \pmod{p}.$$

Der allgemeine Fall.

§ 15. Die Kongruenz (II) kann weiter durch

$$\Sigma G_j Y_j \equiv 0 \pmod{\Phi^{(m-1)}, \Phi^{(l)}, (P^{(k)})} \qquad \text{(III)}$$

ersetzt werden, wo $(\Phi^{(m-1)})_{x_l = \alpha_l}$ eine in dem durch Adjunktion einer Wurzel $x_l \equiv \alpha_l$ der Kongruenz $\Phi^{(l)} \equiv 0 \pmod{(P^{(k)})}$ entstandenen Gattungsbereich $((l-1), \alpha_l) \pmod{(P^{(k)})}$ irreduzible Form bedeutet, die x_{m-1} wirklich enthält, und in der der Koeffizient der höchsten Potenz von x_{m-1} eine mod. $(P^{(k)})$ von 0 verschiedene rationale und ganze Form der Unbestimmten $x_1, \ldots, x_{l-1}$ ist.

Wie man (II) auf (III) reduziert, ist näher auseinanderzusetzen. Zu diesem Zwecke schreiben wir (II) in der Gestalt

$$\Psi Y + \Sigma G_j Y_j \equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})}. \qquad \text{(IIa)}$$

Ψ enthält wenigstens eine der Unbestimmten $x_{l+1}, \ldots, x_{m-1}$, da wir es sonst mit einem schon erledigten Probleme zu tun haben. In dem durch Adjunktion einer Wurzel $x_l \equiv \alpha_l$ der Kongruenz $\Phi^{(l)} \equiv 0 \pmod{(P^{(k)})}$ entstandenen Gattungsbereiche $((l-1), \alpha_l) \pmod{(P^{(k)})}$, wird $(\Psi)_{x_l = \alpha_l}$ nicht verschwinden, da sonst auch Ψ durch $\Phi^{(l)}$ teilbar mod. $(P^{(k)})$ wäre.

Wenn weiter in $(\Psi)_{x_l = \alpha_l}$ keine der Unbestimmten $x_{l+1}, \ldots, x_{m-1}$ wirklich vorkommt, d. h.

$$(\Psi)_{x_l = \alpha_l} \equiv \frac{\varphi(x_1, \ldots, x_{l-1}, \alpha_l)}{\psi(x_1, \ldots, x_{l-1}, \alpha_l)} \pmod{(P^{(k)})}$$

ist, so muß auch

$$\psi(x_1, \ldots, x_l)\, \Psi \equiv \varphi(x_1, \ldots, x_{l-1}, x_l) \pmod{\Phi^{(l)}, (P^{(k)})}$$

sein, und die gegebene Kongruenz geht dann durch Multiplikation mit ψ, die an der Problemstellung nichts ändert, in

$$\varphi Y + \Sigma G_j (\psi Y_j) \equiv 0 \pmod{\Phi^{(l)}, P^{(k)}}$$

über. Diese Kongruenz ist aber vollständig gelöst, da zuerst in Bezug auf die Unbekannten Y, ψY_j zwei Koeffizienten φ

und $\Phi^{(l)}$ nur mehr die Unbestimmten $x_1, \ldots, x_l$ enthalten, und dasselbe für jene weiteren Kongruenzen

$$\psi Y_j \equiv \Sigma G_s U_s + \Phi^{(l)} Z \pmod{(P^{(k)})}$$

der Fall ist, aus denen Y_j zu bestimmen ist.

Wir haben uns also nur noch mit dem Falle zu beschäftigen, wo $(\Psi)_{x_l = \alpha_l}$ eine der Unbestimmten $x_{l+1}, \ldots, x_{m-1}$ wirklich enthält. Da aber $l > k + 1$, gibt es eine homogene lineare Transformation, deren Determinante Eins und deren Koeffizienten rationale und ganze Formen der Unbestimmten $x_1, \ldots, x_{l-1}$ sind, die $(\Psi)_{x_l = \alpha_l}$ in eine reguläre Form von $x_{l+1}, \ldots, x_{m-1}$ überführt, und dieselbe Transformation führt Ψ in eine reguläre Form von $x_{l+1}, \ldots, x_{m-1}$ über, deren Koeffizienten rationale und ganze Formen von $x_1, \ldots, x_l$ sind, wo aber, der Bestimmung dieser Transformation entsprechend, der Koeffizient der höchsten Potenz von x_{m-1} nicht teilbar mod. $(P^{(k)})$ durch $\Phi^{(l)}$ sein kann*). Es wird also nach der Transformation:

$$\Psi = \psi x_{m-1}^{r} + \cdots$$

Da nun jene Transformation wieder an der Problemstellung nichts ändert, können wir unbeschadet der Allgemeinheit Ψ in dieser Gestalt voraussetzen. Es ist aber für die Resultante von ψ und $\Phi^{(l)}$ nach x_l:

$$\lambda \psi + \mu \Phi^{(l)} \equiv \Phi^{(l-1)} \pmod{(P^{(k)})}$$

$\Phi^{(l-1)}$ eine mod. $(P^{(k)})$ von 0 verschiedene Form, die nur mehr die Unbestimmten $x_1, \ldots, x_{l-1}$ enthalten kann. Fügt man demnach in (IIa) den Faktor λ hinzu, was wieder an der Aufgabe nichts ändert, so wird diese

*) Betrachtet man nämlich Ψ als Form der Unbestimmten $x_{l+1}, \ldots, x_{m-1}$, so wird jeder ihrer Koeffizienten, wie überhaupt jede Form der Unbestimmten $x_1, \ldots, x_l$ durch die Substitution $x_l = \alpha_l$ dann und nur dann $\equiv 0 \pmod{(P^{(k)})}$ werden, wenn diese Form ursprünglich schon $\equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})}$ war. Es kann also jedes Glied von Ψ, dessen Koeffizient $\equiv 0 \pmod{\Phi^{(l)}, (P^{(k)})}$ ist, oder also nach der Substitution $x_l = \alpha_l \pmod{(P^{(k)})}$ verschwindet, von Anfang an weggelassen werden.

$$(\Phi^{(l-1)}x_{m-1}^{\nu}+\cdots)\,Y+\Sigma G_j(\lambda Y_j)\equiv 0\ \left(\text{mod. }\Phi^{(l)},(P^{(k)})\right),$$

die bis auf die Irreduzibilität*) des Koeffizienten von Y in Bezug auf die Unbekannten $Y, \lambda Y_j$ die in (III) postulierte Gestalt besitzt, während die zur endgültigen Lösung noch weiter zu behandelnden Kongruenzen

$$\lambda Y_j\equiv\Sigma G_s U_s+\Phi^{(l)}Z\ \left(\text{mod. }(P^{(k)})\right),$$

da λ und $\Phi^{(l)}$ nur mehr die Unbestimmten $x_1,\ldots,x_l$ enthalten, und λ nicht teilbar $\left(\text{mod. }(P^{(k)})\right)$ durch $\Phi^{(l)}$ ist, als erledigt betrachtet werden können.

§ 16. Die dargelegte Reduktionsmethode wird vollständig, wenn wir die Lösung der allgemeinen Kongruenz

$$\Sigma F_j X_j\equiv 0\ \left(\text{mod. }\Phi^{(m-1)},\ldots,\Phi^{(r)},\Phi^{(l)},(P^{(k)})\right)\qquad\text{(I)}$$

für $r=l+1$ auf erledigte Probleme, für $r>l+1$ auf die Lösung von

$$\Sigma G_j Y_j\equiv 0\ \left(\text{mod. }\Psi^{(m-1)},\ldots,\Psi^{(r)},\Psi^{(r-1)},\Psi^{(l)},(P^{(k)})\right)\qquad\text{(II)}$$

zurückführen, soweit dabei nicht der besonders zu behandelnde „singuläre Fall" auftritt. ($\Phi^{(l)}$ besitzt die zu Beginn des § 14 geforderten Eigenschaften.)

Dabei soll immer $\Phi^{(i)}(i=r,\ldots,m-1)$ eine Form bedeuten, die $x_{i+1},\ldots,x_m$ nicht, wohl aber x_i wirklich enthält, in welcher der Koeffizient der höchsten Potenz von x_i nur mehr die Unbestimmten $x_1,\ldots,x_{l-1}$ enthält, und die, wenn man $x_l=\alpha_l, x_r=\alpha_r,\ldots,x_{i-1}=\alpha_{i-1}$ setzt, in dem Gattungsbereiche $((l-1),\alpha_l,x_{l+1},\cdots,x_{r-1},\alpha_r,\cdots,\alpha_{i-1})$ $\left(\text{mod. }(P^{(k)})\right)$ irreduzibel ist. Dieser Gattungsbereich (mod. $P^{(k)}$) entsteht

*) Daß man den Koeffizienten von Y, wenn $x_l=\alpha_l$ gesetzt wird, als in dem Gattungsbereiche $\left((l-1),\alpha_l\right)$ $\left(\text{mod. }(P^{(k)})\right)$ irreduzibel annehmen kann, ist, um Wiederholungen zu vermeiden, hier übergangen; der Beweis findet sich bei der sogleich (§ 18) zu erörternden allgemeinen Darstellung dieses Reduktionsverfahrens.

durch successive Adjunktion der Wurzel $x_l = \alpha_l$, der Kongruenz $\Phi^{(l)} \equiv 0$, der Wurzel $x_r = \alpha_r$ der Kongruenz

$$\Phi(x_r, \ldots, \alpha_l, \ldots) \equiv 0, \text{ u. s. f.}$$

Die postulierten Eigenschaften der Formen Ψ sind wegen der neu eingeschalteten Form $\Psi^{(r-1)}$ in (II) entsprechend zu modifizieren, indem man $r - 1$ statt r setzt.

Der Fall, wo die Unbestimmte x_m in keinem der Koeffizienten F von (I) wirklich vorkommt, ist nach § 11 wieder als erledigt zu betrachten.

Ist ein F vorhanden, das die Unbestimmte x_m wirklich enthält, so sei z. B. F_1 vom niedrigsten, μ^{ten} Grade in x_m, wo μ aber auch 0 sein kann. Dabei kommen nur solche Koeffizienten in Betracht, die nicht

$$\equiv 0 \ \left(\text{mod. } \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right)$$

sind. Insbesondere muß dies auch für $F_{1\mu}$ in

$$F_1 = F_{1\mu} x_m^{\mu} + \cdots$$

der Fall sein. Trotzdem kann aber jetzt

$$(F_{1\mu})_{x_l = \alpha_l, x_r = \alpha_r, \cdots, x_{m-1} = \alpha_{m-1}} \ \left(\text{mod. } (P^{(k)})\right)$$

verschwinden. Dann gibt es aber nach § 9 eine mod. $(P^{(k)})$ nicht verschwindende Form $\Phi^{(l-1)}$ der Unbestimmten $x_1, \ldots, x_{l-1}$ von der Beschaffenheit, daß

$$\Phi^{(l-1)} F_{1\mu} \equiv 0 \ \left(\text{mod. } \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right)$$

wird, wo $\Phi^{(l-1)}$ durch Auflösung von linearen diophantischen Gleichungen in $[[1], x_1, \ldots, x_{m-1}]$ völlig bestimmt ist. Die Kongruenz (I), die auch

$$\sum_{j=1}^{h} F_j X_j + \sum_{i=r}^{m-1} \Phi^{(i)} Y_i + \Phi^{(l)} Y_l \equiv 0 \text{ mod. } (P^{(k)})$$

geschrieben werden kann, wird durch Multiplikation mit $\Phi^{(l-1)}$:

$$(\Phi^{(l-1)} F_1) X_1 + \sum_{j=2}^{h} F_j (\Phi^{(l-1)} X_j) + \sum_{i=r}^{m-1} \Phi^{(i)} (\Phi^{(l-1)} Y_i) + \\ + \Phi^{(l)} (\Phi^{(l-1)} Y_l) \equiv 0 \ \left(\text{mod. } (P^{(k)})\right),$$

die (I) vollständig ersetzt, da, wenn die Unbekannten $\Phi^{(l-1)} X_j, \ldots$

bestimmt sind, hieraus auch die Unbekannten X_j, deren Koeffizienten nur mehr von $x_1, \ldots, x_{l-1}$ abhängen, bestimmt werden können.

Man gelangt demnach schließlich zu einer Kongruenz (I), in welcher, wenn z. B. der Koeffizient F_1 vom niedrigsten, μ^{ten} Grade in x_m ist, die durch

$$F_1 = F_{1\mu} x_m^\mu + \cdots$$

definierte Größe $F_{1\mu}$ so beschaffen ist, daß

$$(F_{1\mu})_{x_l = a_l, x_r = a_r, \cdots, x_{m-1} = a_{m-1}} \left(\text{mod. } (P^{(k)})\right)$$

nicht verschwindet. (Ausgenommen ist nur der Fall, wo schließlich alle $F \equiv 0$ werden, und demnach die Kongruenz wieder schon erledigt ist.)

Dann kann man aber nach § 9 eine zweite Form $G_{1\mu}$ bestimmen, so daß

$$(G_{1\mu})_{x_l = a_l, x_r = a_r, \cdots, x_{m-1} = a_{m-1}} \left(\text{mod. } (P^{(k)})\right)$$

wieder von 0 verschieden, und

$$F_{1\mu} G_{1\mu} \equiv \Phi^{(r-1)} \left(\text{mod. } \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right)$$

ist, und $\Phi^{(r-1)}$ nur mehr die Unbestimmten $x_1, \ldots, x_{l-1}, x_{l+1}, \ldots, x_{r-1}$ enthält.

In der Kongruenz

$$G_{1\mu} \sum_{j=1}^{h} F_j X_j \equiv 0 \left(\text{mod. } \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right) \qquad \text{(III)}$$

wird daher, wenn man $G_{1\mu} F_1$ nach Potenzen von x_m ordnet, der Koeffizient von x_m^μ jetzt $\Phi^{(r-1)}$ sein, und es ist $G_{1\mu} F_1$ auch jetzt jener Koeffizient, der den niedrigsten Grad in x_m besitzt.

§ 17. Das Problem der Auflösung von (III) ist aber, bis auf als erledigt zu betrachtende Probleme niedrigeren Ranges, mit dem Probleme (I) völlig gleichwertig.

Jede Lösung von (I) ist auch eine Lösung von (III). Aus den Lösungen von (III) enthält man auch umgekehrt die Lösungen von (I) auf folgendem Wege. Ist für irgend ein Formensystem X_j:

$$G_{1\mu} \sum_{j=1}^{h} F_j X_j \equiv 0 \ \left(\text{mod. } \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right),$$

so ist auch

$$\left(\sum_{j=1}^{h} F_j X_j\right)_{x_l = \alpha_l, x_r = \alpha_r, \cdots, x_{m-1} = \alpha_{m-1}} \equiv 0 \ \left(\text{mod. } (P^{(k)})\right),$$

und es gibt eine nach § 9 bekannte Form $\Phi^{(l-1)}$ der Unbestimmten $x_1, \ldots, x_{l-1}$, so daß

$$\Phi^{(l-1)} \sum_{j=1}^{h} F_j X_j \equiv 0 \ \left(\text{mod. } \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right)$$

oder auch

$$\Phi^{(l-1)} \sum_{j=1}^{h} F_j X_j + \sum_{i=r}^{m-1} \Phi^{(i)} Y_i + \Phi^{(l)} Y_l \equiv 0 \ \left(\text{mod. } (P^{(k)})\right)$$

wird. Soll aber jenes Formensystem X_j auch eine Lösung von (I) sein, so muß ferner eine Relation

$$\Phi^{(l-1)} \sum_{j=1}^{h} F_j X_j + \sum_{i=r}^{m-1} \Phi^{(i)} \Phi^{(l-1)} Z_i + \Phi^{(l)} \Phi^{(l-1)} Z_l \equiv 0 \ \left(\text{mod.} (P^{(k)})\right)$$

bestehn. Augenscheinlich hat man hierfür die notwendige und hinreichende Bedingung

$$\sum_{i=r}^{m-1} \Phi^{(i)} (Y_i - \Phi^{(l-1)} Z_i) + \Phi^{(l)} (Y_l - \Phi^{(l-1)} Z_l) \equiv 0 \ \left(\text{mod.} (P^{(k)})\right), \quad \text{(IV)}$$

deren Lösung nach den Unbekannten $Y_i - \Phi^{(l-1)} Z_i$, $Y_l - \Phi^{(l-1)} Z_l$ bekannt ist.

Die allgemeine Lösung von (III) ergibt

$$X_j \equiv \sum G_{js} U_s \ \left(\text{mod. } (P^{(k)})\right)$$

und hieraus weiter

$$Y_i \equiv \sum H_{is} U_s \ \left(\text{mod. } (P^{(k)})\right)$$

$$Y_l \equiv \sum H_{ls} U_s \ \left(\text{mod. } (P^{(k)})\right).$$

Man hat dann weiter

$$Y_i - \Phi^{(l-1)} Z_i \equiv \sum K_{it} V_t \ \left(\text{mod. } (P^{(k)})\right)$$

und, da hier ein Koeffizient $\Phi^{(l-1)}$ vorkommt, die nähere Bestimmung der U_s, so daß endlich

$$X_j \equiv \sum G_{js} U_s, \quad U_s \equiv \sum G'_{st} W_t \ \left(\text{mod. } (P^{(k)})\right)$$

die allgemeine Lösung von (I) darstellt.

Damit ist aber die Lösung von (I) für den Fall, wenn ein Koeffizient F vom Grade 0 in x_m ist, auf die Lösung von III zurückgeführt.

Enthält ein F die Unbestimmte x_m, während alle andern Koeffizienten

$$\equiv 0 \ \left(\text{mod. } \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right)$$

sind, so haben wir es mit der Kongruenz

$$FX + \sum_{i=r}^{m-1} \Phi^{(i)} Y_i + \Phi^{(l)} Y^{(l)} \equiv 0 \ (\text{mod. } P^{(k)})$$

zu tun, die den allgemeinen Typus des — zuletzt gesondert zu behandelnden — singulären Falls darstellt.

Endlich können alle F, deren Anzahl nun > 1 angenommen werden kann, die Unbestimmte x_m enthalten. Dann führt aber das für die Reduktion des Grades der F in x_m schon in § 14 zur Anwendung gekommene Verfahren entweder zum singulären Fall, oder aber zu Kongruenzen, die bis auf die Irreduzibilität der Φ von der Gestalt (II) sind, und dasselbe ist für die inzwischen aufzulösenden Kongruenzen der Fall.

Der Fall, wo $\Phi^{(r-1)}$ nur mehr $x_1, \ldots, x_l$ enthält, führt unmittelbar auf ein schon erledigtes Problem niedrigeren Ranges. Dies ist unter anderm stets für $r = l + 1$ der Fall.

Wenn $\Phi^{(r-1)}$ wenigstens eine der Unbestimmten $x_{l+1}, \ldots, x_{r-1}$ wirklich enthält, so ist noch nachzuweisen, daß wir uns auf die Annahme beschränken können, daß die neu eingeführte Form $\Phi^{(r-1)}$ die Unbestimmte x_{r-1} wirklich enthält, und der Koeffizient der höchsten Potenz von x_{r-1} nur mehr die Unbestimmten $x_1, \ldots, x_{l-1}$ enthält.

Wegen $l > k + 1$ gibt es aber (in genauer Wiederholung der am Ende des § 15 angewandten Schlußweise) eine homogene lineare Transformation, deren Determinante gleich Eins, und deren Koeffizienten rationale und ganze Formen der Unbestimmten $x_1, \ldots, x_{l-1}$ sind, die $(\Phi^{(r-1)})_{x_l = \alpha_l}$ in eine reguläre Form von $x_{l+1}, \ldots, x_{r-1}$ überführt; und dieselbe Transformation führt $\Phi^{(r-1)}$ in eine reguläre Form von $x_{l+1}, \ldots, x_{r-1}$ über, deren Koeffizienten rationale und ganze Formen von $x_1, \ldots, x_l$ sind; wo aber den getroffenen Bestimmungen entsprechend, der Koeffizient der höchsten Potenz von x_{r-1} nicht teilbar mod. $(P^{(k)})$ durch $\Phi^{(l)}$ sein kann.

Da nun diese Transformation an der Problemstellung und auch an der postulierten Beschaffenheit der Formen $\Phi^{(r)}, \ldots, \Phi^{(m-1)}$ nichts ändert, können wir unbeschadet der Allgemeinheit $\Phi^{(r-1)}$ in dieser Gestalt voraussetzen, und wenn wir die Kongruenz

$$\sum_{j=1}^{h} F_j X_j + \sum_{i=r}^{m-1} \Phi^{(i)} Y_i + \Phi^{(r-1)} Y_{r-1} \equiv 0 \left(\text{mod. } \Phi^{(l)}, (P^{(k)})\right)$$

schreiben, genau so wie an der eben angeführten Stelle den Koeffizienten Y_{r-1} endgültig auf die verlangte Gestalt bringen.

An der Auflösung der vorgelegten Kongruenz tritt hierbei nur die Änderung ein, daß jetzt die „Unbekannten" λX_j, λY_i auftreten, aus denen aber auch X_j, Y_i sich unmittelbar bestimmen lassen, da ja λ eine Form von $x_1, \ldots, x_l$ allein ist, die mod. $(P^{(k)})$ nicht durch $\Phi^{(l)}$ teilbar ist, wir es also mit solchen Kongruenzen zu tun haben, in denen zwei von 0 $\left(\text{mod. } (P^{(k)})\right)$ verschiedene Koeffizienten Formen von $x_1, \ldots, x_l$ allein sind.

§ 18. Die arithmetische Theorie der linearen diophantischen Probleme wird daher — abgesehn vom singulären Falle — vollständig erledigt sein, wenn wir noch die Kongruenz

$$\sum_{j=1}^{h} F_j X_j \equiv 0 \left(\text{mod. } \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right) \quad \text{(C)}$$

auf eine solche zurückführen, in der die Φ die zu Beginn des

§ 16 postulierte Irreduzibilitätseigenschaft besitzen. Denn man gelangt dann durch die angegebenen Methoden schließlich zu $r = l + 1$, in welchem Falle die Kongruenz als vollständig erledigt angenommen werden kann.

Ist z. B. $\Phi^{(s)}$ $(r \leqq s \leqq m-1)$ die erste Form in der Reihe $\Phi^{(r)}, \ldots, \Phi^{(m-1)}$, die für $s > r$ in dem Gattungsbereiche $((l-1), \alpha_l, \ldots, \alpha_{s-1})$ $\left(\text{mod. } (P^{(k)})\right)$ für $s = r$ im Gattungsbereiche $((l-1), \alpha_l)$ $\left(\text{mod. } (P^{(k)})\right)$ nicht irreduzibel ist, so möge

$$(\Phi^{(s)})_{x_l=\alpha_l, \cdots, x_{s-1}=\alpha_{s-1}} = (\Phi_1^{(s)})_{x_l=\alpha_l, \cdots, x_{s-1}=\alpha_{s-1}} \cdots$$

die Zerlegung dieser Größe in irreduzible Faktoren in jenem Gattungsbereiche darstellen. Die rechts auftretenden Nenner sind $\left(\text{mod. } (P^{(k)})\right)$ von 0 verschiedene rationale und ganze Formen von $x_1, \ldots, x_{l-1}, x_{l+1}, \ldots, x_{r-1}$. Es gibt demnach eine ebensolche rationale und ganze Form dieser Unbestimmten, die mit $\Psi^{(r-1)}$ bezeichnet werden mag, so daß

$$\Psi^{(r-1)}\Phi^{(s)} \equiv \Phi_1^{(s)}\Phi_2^{(s)} \ldots \left(\text{mod. } \Phi^{(s-1)}, \ldots, \Phi^{(l)}, (P^{(k)})\right),$$

wo die $\Phi_1^{(s)}, \Phi_2^{(s)}, \ldots$ nach jener Substitution im Gattungsbereiche $((l-1), \alpha_l, \ldots, \alpha_{s-1})$ $\left(\text{mod. } (P^{(k)})\right)$ irreduzible, rationale und ganze Formen von $x_1, \ldots, x_{l-1}, x_{l+1}, \ldots, x_{r-1}$ sind.

Jede Lösung von (C) genügt auch der folgenden Kongruenz:

$$\sum_{j=1}^{h} F_j(\Psi^{(r-1)} X_j) + \sum_{i=s+1}^{m-1} \Phi^{(i)}(\Psi^{(r-1)} Y_i) + \Phi_1^{(s)} \cdots Y_s \equiv 0$$
$$\left(\text{mod. } \Phi^{(s-1)}, \cdots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right),$$

und es ist demnach für jedes entsprechende Y_s

$$(\Phi_1^{(s)} \cdots Y_s)_{x_l=\alpha_l, x_r=\alpha_r, \cdots, x_{s-1}=\alpha_{s-1}}$$

durch $\Psi^{(r-1)}$ teilbar. Infolge der Irreduzibilität der ersten Faktoren findet dasselbe für $(Y_s)_{x_l=\alpha_l, x_r=\alpha_r, \cdots, x_{s-1}=\alpha_{s-1}}$ statt. Nach früher bewiesenen Sätzen (§ 9 d. Kap. und Kap. VII § 7) gibt es also eine rationale und ganze Form von $x_1, \ldots, x_{l-1}$,

die durch vollständig erledigte Methoden bestimmt ist, $\overline{\Psi}^{(l-1)}$, von der Beschaffenheit, daß

$$\overline{\Psi}^{(l-1)} Y_s \equiv \Psi^{(r-1)} Z_s \left(\text{mod. } \Phi^{(s-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right). \quad (C_1)$$

Jede Lösung von (C) genügt also weiter auch der folgenden Kongruenz:

$$\Psi^{(r-1)}\left(\sum_{j=1}^{h} F_j\left(\overline{\Psi}^{(l-1)} X_j\right) + \sum_{i=s+1}^{m-1} \Phi^{(i)}\left(\overline{\Psi}^{(l-1)} Y_i\right) + \Phi_1^{(s)} \cdots Z_s\right) \equiv 0$$
$$\left(\text{mod. } \Phi^{(s-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right),$$

aus der in wiederholter Anwendung der benutzten Schlußweise auch noch

$$\sum_{j=1}^{h} F_j\left(\Psi^{(l-1)} X_j\right) + \sum_{i=s+1}^{m-1} \Phi^{(i)}\left(\Psi^{(l-1)} Y_i\right) + \Phi_1^{(s)} \cdots \left(\Psi_1^{(l-1)} Z_s\right) \equiv 0$$
$$\left(\text{mod. } \Phi^{(s-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right) \quad (C_2)$$

oder mit Berücksichtigung von (C_1) auch

$$\sum_{j=1}^{h} F_j\left(\Psi^{(l-1)} X_j\right) + \sum_{i=s+1}^{m-1} \Phi^{(i)}\left(\Psi^{(l-1)} Y_i\right) + \Phi^{(s)}\left(\Psi^{(l-1)} Y_s\right) \equiv 0$$
$$\left(\text{mod. } \Phi^{(s-1)}, \cdots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right) \quad (C_3)$$

folgt.

Die Lösung von C_2 in Bezug auf die „Unbekannten“ $\Psi^{(l-1)} X_j$, $\Psi^{(l-1)} Y_i$, $\Psi_1^{(l-1)} Z_s$ erfolgt durch eine Kette von Kongruenzen, in denen die Koeffizienten der letzten Unbekannten der Reihe nach $\Phi_1^{(s)}$, $\Phi_2^{(s)}$, ... sind, wo nun auch $\Phi_1^{(s)}$, $\Phi_2^{(s)}$, ... die Irreduzibilitätseigenschaft besitzen. Diese sind aber als erledigt zu betrachten; hieraus ergeben sich weiter die Lösungen von (C_3), wenn man — durch gleichfalls schon erledigte Methoden — Y_s aus (C_1) bestimmt.

Jede Lösung von C ist in den Lösungen von (C_3) enthalten; soll umgekehrt eine Lösung von (C_3) auch (C) genügen, so muß der aus (C_3) sich ergebende Ausdruck

$$\sum_{j=1}^{h} F_1(\Psi^{(l-1)} X_j) + \sum_{i=s+1}^{m-1} (\Psi^{(l-1)} Y_i) + \Phi^{(s)} \Psi_1^{(l-1)} Y_s \equiv$$

$$\equiv \sum_{h=r}^{s-1} \Phi^{(h)} U_h + \Phi^{(l)} U_1 \quad \left(\text{mod. } (P^{(k)})\right)$$

auch

$$\equiv \Psi^{(l-1)} \left(\sum_{h=r}^{s} \Phi^{(h)} U_h' + \Phi^{(l)} U_1' \right) \quad \left(\text{mod. } (P^{(k)})\right)$$

sein. Dies ergibt durch bekannte Methoden eine weitere Bestimmung der für die Lösung von (C_3) nach beliebigen Formen und endlich aus

$$\Psi^{(l-1)} X_j \equiv \sum_{(i)} G_{ji} W_i$$

die Lösungen von (C).

Mit dem Vorstehenden ist aber unser Problem noch immer nicht vollständig abgeschlossen. Denn die Zerlegung von $\Phi^{(s)}$ in irreduzible Faktoren $\Phi_1^{(s)}, \ldots$ ist wohl erfolgt; aber diese haben nicht mehr die vorausgesetzte Gestalt, indem nun der Koeffizient der höchsten Potenz von x_s nicht bloß $x_1, \ldots, x_{l-1}$, sondern auch $x_{l+1}, \ldots, x_{r-1}$ enthalten kann. Soll dies stattfinden, so muß jedenfalls $r > l+1$ sein, und $s > r$ sein; da aber andrerseits $l \geqq 1$ ist, folgt hieraus $s \geqq 4$; wegen $s \leqq m-1$ kann dies also nur für $m \geqq 5$ stattfinden.

Das Problem der homogenen linearen diophantischen Gleichung ist demnach — (den singulären Fall behandeln wir in § 19) — auch für die Bereiche $[[1], x_1, x_2, x_3]$ und $[[1], x_1, x_2, x_3, x_4]$ vollständig erledigt.

Um nun zu den Fällen, wo mehr als vier Unbestimmte vorhanden sind, aufzusteigen, sind die grundlegenden Sätze in § 9 entsprechend zu verallgemeinern. Hierzu bietet eine homogene lineare Transformation der Unbestimmten $x_1, \ldots, x_{l-1}$, $x_{l+1}, \ldots, x_{r-1}, x_s$ das passende Mittel. Wenn auch das so entstehende Formensystem durchaus nicht so einfach ist, wie in dem durchgeführten Falle, bleibt doch der Gedankengang

im Wesen derselbe. Mit Rücksicht auf die große Komplikation sehe ich von einer ausführlichen Darstellung ab, um so mehr, als eine tatsächliche Anwendung dieser Resultate für mehr als vier Unbestimmte vorderhand wohl kaum in Aussicht genommen werden kann.

Der singuläre Fall.

§ 19. Die Auflösung der homogenen linearen diophantischen Gleichung wird immer durch eine endliche Reihe von Operationen geleistet sein, wenn wir dasselbe noch für den singulären Fall

$$FX + \Phi^{(m-1)} Y_{m-1} + \cdots + \Phi^{(r)} Y_r + \Phi^{(l)} Y_l \equiv 0 \pmod{P^{(k)}} \quad (S)$$

durchführen, wo die Formen Φ schon die § 16 auseinandergesetzte Irreduzibilitätseigenschaft besitzen*). Dann muß aber

$$(FX)_{x_l = \alpha_l, x_r = \alpha_r, \cdots, x_{m-1} = \alpha_{m-1}} \equiv 0 \left(\mathrm{mod.}\ (P^{(k)})\right)$$

sein, und es gibt demnach eine nach den bisherigen Auseinandersetzungen durch eine endliche Reihe von Operationen bestimmte Form $\Psi^{(l-1)}$ der Unbestimmten $x_1, \ldots, x_{l-1}$, so daß entweder

$$\Psi^{(l-1)} F \equiv 0 \left(\mathrm{mod.}\ \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right) \quad (a)$$

wird, oder aber

$$\Psi^{(l-1)} X \equiv 0 \left(\mathrm{mod.}\ \Phi^{(m-1)}, \ldots, \Phi^{(r)}, \Phi^{(l)}, (P^{(k)})\right) \quad (b)$$

sein muß.

Im ersten Falle kann aber auch die Darstellung

$$\Psi^{(l-1)} F \equiv G_{m-1} \Phi^{(m-1)} + \cdots + G_r \Phi^{(r)}) + G_l \Phi^{(l)} \left(\mathrm{mod.}\ (P^{(k)})\right)$$

durch eine endliche Reihe von Operationen wirklich gegeben werden, und die vorgelegte Kongruenz ist mit

*) Auch hier bezieht sich die Darstellung explicite nur auf den Fall, wo die Anzahl der Unbestimmten nicht größer als vier ist.

$$\Phi^{(m-1)}(\Psi^{(l-1)}Y_{m-1}+G_{m-1}X)+\cdots+\Phi^{(r)}(\Psi^{(l-1)}Y_r+G_rX)+$$
$$+\Phi^{(l)}(\Psi^{(l-1)}Y_l+G_lX)\equiv 0 \ \left(\mathrm{mod.}\,(P^{(k)})\right)$$

zugleich gelöst. Diese ist aber für die Unbekannten $\Psi^{(l-1)}Y_{m-1}+G_{m-1}X, \cdots$ unmittelbar gelöst, weil die Koeffizienten die Unbestimmte x_m überhaupt nicht enthalten; und die sich weiter ergebenden Kongruenzen

$$\Psi^{(l-1)}Y_{m-1}+G_{m-1}X\equiv\sum H_s^{(1)}U_s \ \left(\mathrm{mod.}\,(P^{(k)})\right)$$
$$\Psi^{(l-1)}Y_{m-2}+G_{m-2}X\equiv\sum H_s^{(2)}U_s \ \left(\mathrm{mod.}\,(P^{(k)})\right)$$

bieten wieder nur Probleme niedrigeren Ranges, die als erledigt betrachtet werden können. In jeder von ihnen findet sich nämlich eine neue Unbekannte, deren Koeffizient nur mehr $x_1, \ldots, x_{l-1}$ enthält.

Im zweiten Falle muß jedenfalls der Kongruenz (b) genügt werden. Diese bietet aber wieder wegen des Koeffizienten $\Psi^{(l-1)}$ von X ein schon gelöstes Problem, d. h. es ergibt sich aus ihr jedenfalls für X die notwendige Gestalt

$$X\equiv\sum G_sU_s \ \left(\mathrm{mod.}\,(P^{(k)})\right)$$

und dann

$$\Psi^{(l-1)}X\equiv\sum G_s\Psi^{(l-1)}U_s \ \left(\mathrm{mod.}\,(P^{(k)})\right),$$

wo aber nun

$$G_s\Psi^{(l-1)}\equiv H_{s,m-1}\Phi^{(m-1)}+\cdots+H_{sr}\Phi^{(r)}+H_{sl}\Phi^{(l)} \ \left(\mathrm{mod.}\,(P^{(k)})\right)$$

sein muß, und die wirkliche Darstellung von $G_s\Psi^{(l-1)}$ in dieser Gestalt wieder durch Auflösung von linearen diophantischen Gleichungen in $[[1], x_1, \ldots, x_{m-1}]$ erbracht werden kann.

Die Kongruenz (S) wird demnach, wenn man noch den Faktor $\Psi^{(l-1)}$ hinzufügt, was an ihrer Auflösung nichts ändert:

$$\Phi^{(m-1)}(\Psi^{(l-1)}Y_{m-1}+\sum_{(s)}H_{s,m-1}FU_s)+\cdots+$$
$$+\Phi^{(l)}(\Psi^{(l-1)}Y_l+\sum_{(s)}H_{sl}FU_s)\equiv 0 \ \left(\mathrm{mod.}\,(P^{(k)})\right),$$

woraus wieder zuerst die „Unbekannten“

$$\mathfrak{P}^{(l-1)} Y_{m-1} + \sum_{(s)} H_{s,m-1} F U_s, \cdots$$

berechnet werden können, und dann weiter sich, auf Grundlage von als erledigt anzusehenden Problemen niedrigeren Ranges $Y_{l-1}, \ldots, Y_{m-1}$, eine immer engere Bestimmung der U und schließlich auch X ergibt.

Besteht die Kongruenz (S) nur aus zwei Gliedern, so ist, wie schon früher zu Ende des § 14 erwähnt wurde, diese allgemeine Methode überflüssig, und die Auflösung ergibt sich in elementarer Weise.

Neuntes Kapitel.

Die ganzen algebraischen Größen*).

Einleitende Festsetzungen.

§ 1. Es sei A ein beliebiger orthoider Bereich, oder aber der Bereich [1]. Unsren weiteren Untersuchungen werde wieder der Bereich [A, x_1, x_2, ..., x_m] zu Grunde gelegt, d. h. der Bereich der aus A entstammenden orthoiden, resp. der rationalen und ganzen Formen von m Unbestimmten $x_1, \ldots, x_m$, wo die x neue, d. h. in der Definition des Bereichs A

*) Die Grundlage der Theorie der ganzen algebraischen Größen ist vor allem der Begriff der idealen Größen, die E. E. Kummer zuerst eingeführt hat. („Zur Theorie der complexen Zahlen", Journ. f. r. u. a. Mathematik, Bd. 35. 1847.) Die Definition der idealen Größe, wenn sie bei Kummer auch nur an dem verhältnismäßig einfachen, aber doch durchaus charakteristischen Beispiele der aus dem Probleme der Kreisteilung entstehenden algebraischen Zahlen erfolgt, bedeutet einen epochalen Wendepunkt in der Geschichte der Arithmetik. Die damit begründete Einsicht erreicht aber ihre Vollkommenheit erst durch die in der „Festschrift" (1882) entwickelten Kroneckerschen Methoden, deren Wesen in der Association neuer Unbestimmter beruht. Auf diesen baut sich unsre Darstellung auf. Wie weit sie über die „Festschrift" hinausgeht, wird später im einzelnen nachzuweisen sein. Die Hauptpunkte der weiteren Entwicklung sind folgende: Die im früheren gegebene vollständige Lösung der linearen diophantischen Probleme, die an Stelle der begrifflichen Definition der neu auftretenden Gebilde ihre tatsächliche Darstellung setzt; die Definition der idealen Größen als dem gewöhnlichen Additions- und Multiplikationsgesetz unterworfener Größen; die dementsprechende Aufstellung eines „Fundamentalsystems" der idealen ganzen Größen; die Ergänzung der Kroneckerschen Resultate

nicht verwendete Unbestimmte sind. Es entstehen dadurch wieder, wie in den vorhergehenden Kapiteln, zwei parallele Theorien, die eine algebraischen, die andere arithmetischen Charakters, deren Grundzüge gemeinschaftlich vorgetragen werden können; ein Umstand, der die ganze Darstellung nicht nur kürzer, sondern auch durchsichtiger gestaltet.

Wenn sich zum Schluß die beiden Theorien wieder trennen, erhalten wir bei der ersten Annahme eine im Geiste der Arithmetik gehaltene Theorie der algebraischen Funktionen, insbesondere, wenn in die Definition von A keinerlei Unbestimmte eintreten, die einer geometrischen Interpretation fähigen Sätze dieser Theorie. Die zweite Annahme, $\mathsf{A} = [1]$, ergibt die allgemeinsten Begriffsbildungen der reinen Arithmetik, die große Schöpfung Kroneckers, die arithmetische Theorie der algebraischen Größen.

Es seien $F_0, F_1, \ldots, F_n$ irgend welche Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$*), und endlich

$$F(z) = F_0 z^n + F_1 z^{n-1} + \cdots + F_n = 0$$

eine in $(\mathsf{A}, x_1, \ldots, x_m)$ irreduzible Gleichung. Adjungiert man dem Bereiche $(\mathsf{A}, x_1, \ldots, x_m)$ eine Wurzel α der Gleichung

---

für jene natürlichen Primzahlen, die den Methoden der Festschrift entgehn; und endlich die Richtigstellung der Kroneckerschen Sätze über die einem Gattungsbereich entsprechende Zerlegung der ganzen Größen in Primideale.

Die allgemeine Theorie der algebraischen Zahlen hat — zeitlich viel früher, zuerst in der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie (1871) und in einer Reihe weiterer glänzender Abhandlungen — R. Dedekind durch wohl weniger einfache, aber um so scharfsinnigere Methoden begründet, die dann von ihm und H. Weber „Theorie der algebraischen Funktionen einer Veränderlichen", Journ. f. r. u. a. Math., Bd. 92, 1881) auf das im Citat genannte Gebiet übertragen wurden.

Diese Arbeit behandelt die Theorie der algebraischen Funktionen, von den Zahlenkoeffizienten abgesehn. Die im vollen Sinne des Wortes „arithmetische" Theorie der algebraischen Größen ist Kroneckers Schöpfung.

*) Es kann auch $m = 0$ sein; in diesem Falle sind die F Größen des Bereichs A.

$F(z) = 0$, so entsteht ein Gattungsbereich, der kurz mit Γ bezeichnet werden soll. Der Gattungsbereich Γ umfaßt alle Größen von der Gestalt:

$$g(\alpha) = \frac{G_0 + G_1\alpha + \cdots + G_{n-1}\alpha^{n-1}}{H},$$

wo $G_0, G_1, \ldots, G_{n-1}, H$ bis auf die Bedingung $H \neq 0$ beliebige Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ sind.

Die (auf die additive und multiplikative Verknüpfung bezüglichen) „Eigenschaften" des Gattungsbereichs Γ sind von der weiteren Interpretation der Größe α unabhängig. Bildet man insbesondere den Galoisschen Bereich der Gleichung $F(z) = 0$, und sind $\alpha_1, \ldots, \alpha_n$ die Wurzeln dieser Gleichung in diesem Bereiche, ferner $\Gamma_1, \ldots, \Gamma_n$ die diesen entsprechenden konjugierten Gattungsbereiche, so werden die für α und Γ gültigen Folgerungen auch für irgend ein α_i und Γ_i richtig bleiben; und wir werden umgekehrt, wo es sich um irgend ein α_i und Γ_i handelt, auch α und Γ schreiben können.

Die Größen des Gattungsbereichs Γ sind „in Bezug auf A" algebraische, (wenn $\mathsf{A} = [1]$, absolut algebraische) Größen, deren Ordnung n oder ein Teiler von n ist. Insbesondere sind die in Γ enthaltenen Größen erster Ordnung Quotienten von der Gestalt $\frac{G_0}{H}$, die wir auch als in Bezug auf $[\mathsf{A}, x_1, \ldots, x_m]$ rationale Größen des Bereichs Γ bezeichnen wollen.

Mit $g(\alpha)$ sind auch die Größen $g(\alpha_1), \ldots, g(\alpha_n)$ gegeben. Es sei die Norm von $g(\alpha)$ durch

$$\text{Nm. } g(\alpha) = \prod_{i=1}^{n} g(\alpha_i)$$

definiert*), wenn in dem rechts stehenden Ausdruck, der eine symmetrische Form von $\alpha_1, \ldots, \alpha_n$ ist, die der Theorie dieser Formen entsprechende Umrechnung auf Grundlage der Identität

*) Der Ausdruck „Norm" geht für den einfachsten Fall der komplexen ganzen Zahlen noch auf Gauß (1831) zurück.

$$F_0 \prod_{i=1}^{n}(z - \alpha_i) = F_0 z^n + \cdots + F_n$$

stattgefunden hat.

Die Norm jeder Größe des Gattungsbereichs Γ ist eine rationale Größe desselben Bereichs.

Für irgend eine dem Gattungsbereiche Γ entstammende Form

$$\sum_{(r)} g_r(\alpha)\, U_r$$

(die U_r sind wie früher verschiedene Potenzenprodukte der Unbestimmten $u_1, \ldots, u_m$) definieren wir entsprechend:

$$\text{Nm.} \sum_{(r)} g_r(\alpha)\, U_r = \prod_{i=1}^{n} \sum_{(r)} g_r(\alpha_i)\, U_r;$$

es ist demnach die Norm einer aus Γ entstammenden Form eine Form der u, deren Koeffizienten rationale Größen des Bereichs Γ sind.

Der Vollständigkeit wegen sei hier noch bemerkt, daß immer Nm. $(AB) =$ Nm. A Nm. B ist.

Die Form $\sum_{(r)} g_r(\alpha)\, U_r$, die als einfachsten Fall auch die Größen $g(\alpha)$ umfaßt, genügt der Gleichung:

$$\text{Nm.}\left(z - \sum_{(r)} g_r(\alpha)\, U_r\right) = 0.$$

Die Koeffizienten dieser Gleichung sind Formen der u, und die Koeffizienten dieser Formen wieder rationale Größen des Gattungsbereichs Γ.

Die Form Nm. $\left(z - \sum_{(r)} g_r(\alpha)\, U_r\right)$ ist entweder irreduzibel in $(\mathsf{A}, x_1, \ldots, x_m)$, oder die vollständige, d^{te} Potenz einer in $(\mathsf{A}, x_1, \ldots, x_m)$ irreduzibeln Form, wo d einen Teiler von n bedeutet.

Ist nämlich

$$\text{Nm.}\left(z - \sum_{(r)} g_r(\alpha)\, U_r\right) = N_1(z)\, N_2(z) \cdots,$$

so kann man voraussetzen, daß der Koeffizient der höchsten Potenz von z in $N_1(z)$, $N_2(z)$, ... gleich Eins ist, und es muß z. B.

$$N_1(z) = 0$$

eine Wurzel von der Gestalt

$$z = \sum_{(r)} g_r(\alpha_i)\, U_r$$

besitzen, d. h. die Gleichung

$$N_1\left(\sum_{(r)} g_r(z)\, U_r\right) = 0$$

und die Gleichung $F(z) = 0$ haben eine gemeinschaftliche Wurzel α_i. Da aber $F(z) = 0$ irreduzibel ist, muß auch

$$N_1\left(\sum_{(r)} g_r(\alpha_j)\, U_r\right) = 0$$

sein, d. h. der Gleichung $N_1(z) = 0$ genügen alle verschiedenen conjugierten Werte von $\sum_{(r)} g_r(\alpha_i)\, U_r$ und zwar jeder als einfache Wurzel. Es muß also

$$N_1(z) = N_2(z) = \cdots$$

sein, und demnach wird:

$$\text{Nm.}\left(z - \sum_{(r)} g_r(\alpha)\, U_r\right) = (N_1(z))^d.$$

Die ganzen algebraischen Größen und Formen.

§ 2. Die rationalen Größen des Gattungsbereichs Γ, d. h. die Formenquotienten $\frac{G}{H}$ genügen der Gleichung ersten Grades

$$Hz - G = 0,$$

in der noch nach Entfernung des größten gemeinschaftlichen Teilers von G und H immer $(G, H) \sim 1$ vorausgesetzt werden kann. Wenn nach dieser Vereinfachung $H \sim 1$ oder auch $= 1$ geworden, so ist jene rationale Größe eine Form des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ oder — wie wir uns auch aus-

drücken wollen — eine in Bezug auf $[\mathsf{A}, x_1, \ldots, x_m]$ rationale und ganze Größe des Gattungsbereichs Γ. Ist $(H, G) \sim 1$ und H nicht ~ 1, so kann dies selbstverständlich nicht der Fall sein.

Das so für den einfachsten Fall gewonnene Einteilungsprinzip kann unmittelbar auf alle Größen des Gattungsbereichs Γ, sowie auch auf die diesem Gattungsbereiche entstammenden Formen übertragen werden.

Die Größe $g(\alpha)$ und auch die Form $\sum_{(r)} g_r(\alpha)\, U_r$ genügt, wie wir sahen, einer irreduzibeln Gleichung $N_1(z) = 0$, deren Koeffizienten Quotienten von Formen aus $[\mathsf{A}, x_1, \ldots, x_m, u_1, \ldots]$ sind. Entfernt man in dieser Gleichung die Nenner und dann auch den größten gemeinschaftlichen Teiler der als Koeffizienten auftretenden Formen, so entsteht die wieder irreduzible Gleichung

$$G_0 z^d + \cdots + G_d = 0.$$

Ist in dieser Gleichung $G_0 \sim 1$ oder also auch $G_0 = 1$, so soll die Größe $g(\alpha)$ eine ganze algebraische Größe (des Gattungsbereichs Γ), resp. die Form $\sum_{(r)} g_r(\alpha)\, U_r$ eine (dem Gattungsbereiche Γ entstammende) ganze algebraische Form genannt werden. Dabei ist immer (auch später) die nähere Bestimmung „in Bezug auf $[\mathsf{A}, x_1, \ldots, x_m]$“ hinzugefügt zu denken.

Um eine Größe des Gattungsbereichs Γ oder eine diesem entstammende Form als „ganz“ zu erkennen, haben wir den folgenden, mit der eben gegebenen Definition gleichwertigen Satz:

Die Größe $g(\alpha)$, resp. die Form $\sum_{(r)} g_r(\alpha)\, U_r$ ist dann und nur dann ganz, wenn sie irgend einer Gleichung

$$z^d + G_1 z^{d-1} + \cdots + G_d = 0$$

genügt, in der $G_1, \ldots, G_d$ dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$, resp. $[\mathsf{A}, x_1, \ldots, x_m, u_1, \ldots]$ angehörende Formen sind.

Nach der soeben gegebenen Definition der ganzen Größen und Formen ist diese Bedingung jedenfalls notwendig. Wir erkennen sie aber auch als hinreichend, wenn wir bemerken, daß dieselbe Größe (oder Form) jedenfalls der irreduzibeln Gleichung

$$N_1(z) = 0$$

genügt. Schreiben wir diese Gleichung nach Entfernung der Nenner in der Gestalt

$$H_0 z^r + \cdots + H_r = 0,$$

wo auch noch $(H_0, \ldots, H_r) \sim 1$ vorausgesetzt werden kann, so muß

$$z^d + G_1 z^{d-1} + \cdots = (H_0 z^r + \cdots + H_r)(K_0 z^s + \cdots + K_s)$$

sein, wo die H Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m, u_1, \ldots]$ sind. Wäre nun

$$K_i = \frac{K_i'}{K},$$

so hätte man, wenn $(K_0', \ldots, K_s') \sim D$

$$K_i' = DK_i''$$

gesetzt wird,

$$K(z^d + G_1 z^{d-1} + \cdots) = D(H_0 z^r + \cdots)(K_0'' z^s + \cdots),$$

und da die in den Parenthesen stehenden Formen durchweg primitiv sind, weiter $K \sim D$, also auch $H_0 K_0'' \sim 1$, und hieraus endlich, was zu beweisen war, auch $H_0 \sim 1$.

Hieraus ergibt sich weiter der folgende für die Theorie grundlegende Satz:

Summe, Differenz und Produkt zweier ganzer algebraischer Formen sind wieder ganze algebraische Formen.

In diesem Satze sind auch die ganzen algebraischen Größen eingeschlossen, die als spezielle Formen aufgefaßt werden können. Für den Beweis können wir noch voraussetzen, daß die beiden Formen demselben Gattungsbereiche Γ entstammen, da wir immer einen solchen Gattungsbereich

konstruieren können, dem eine beliebige endliche Anzahl algebraischer Größen angehören. Sind nun γ', γ'' die beiden ganzen algebraischen Formen, so hat man nur die Gleichungen

$$\prod_{i=1}^{n}\prod_{j=1}^{n}(z-\gamma_i'\pm\gamma_j'')=0,\quad \prod_{i=1}^{n}\prod_{j=1}^{n}(z-\gamma_i'\gamma_j'')=0$$

zu bilden und erkennt unmittelbar, daß der Koeffizient der höchsten Potenz von z gleich Eins ist, während die übrigen Koeffizienten dem Bereiche A entstammende Formen der x und u sind. Denn sie sind symmetrisch in den γ_i' einerseits und den γ_j'' andrerseits und können demnach so geschrieben werden, daß sie aus A entstammende Formen der x, u und der elementaren symmetrischen Formen der γ_i' und γ_j'' werden, wo die letzteren aber der Annahme nach wieder Formen aus $[\mathsf{A}, x_1, \ldots, x_m, u_1, \ldots]$ sein müssen.

§ 3. Nach dem soeben bewiesenen Satze ist jede Form, deren Koeffizienten ganze Größen aus Γ sind, eine ganze algebraische Form. Es findet aber auch das Umgekehrte statt.

Die Koeffizienten jeder dem Gattungsbereiche Γ entstammenden ganzen algebraischen Form sind ganze algebraische Größen aus Γ.

Ist dies bewiesen, so können wir die „ganzen algebraischen Formen“ — in voller Übereinstimmung mit der bisherigen Anwendung solcher adjektivischer Bezeichnungen — geradezu als solche Formen definieren, deren Koeffizienten ganze algebraische Größen sind.

Für den Beweis des Satzes schreiben wir die im Sinne der ursprünglichen Definition als ganz angenommene Form Φ nach Potenzen einer Unbestimmten geordnet:

$$\Phi=\Phi_0+\Phi_1u_1+\Phi_2u_1^2+\cdots.$$

Sie genügt der Gleichung

$$\mathrm{Nm.}\,(z-\Phi)=0,$$

in welcher der Koeffizient von z^n gleich Eins, die übrigen Koeffi-

zienten der Annahme nach Formen aus $[\mathsf{A}, x_1, \ldots, x_m, u_1, u_2, \ldots]$ sind. Die u_1 nicht enthaltenden Glieder besitzen dieselbe Eigenschaft und ergeben unmittelbar die linke Seite der Gleichung

$$\text{Nm.}\,(z - \Phi_0) = 0,$$

der die Größe Φ_0 genügt. Es ist also Φ_0 und damit auch

$$\Phi - \Phi_0 = u_1(\Phi_1 + \Phi_2 u_1 + \cdots)$$

eine ganze algebraische Form. Diese genügt der Gleichung

$$\text{Nm.}\,(z - u_1(\Phi_1 + \Phi_2 u_1 + \cdots)) = 0$$

oder in ausgeschriebener Gestalt

$$z^n + W_1 z^{n-1} + \cdots + W_n = 0,$$

wo man unmittelbar sieht, daß W_r eine durch u_1^r teilbare Form aus $[\mathsf{A}, x_1, \ldots, x_m, u_1, \ldots]$ ist. Es genügt also

$$\Phi_1 + \Phi_2 u_1 + \cdots$$

der Gleichung

$$t^n + \frac{W_1}{u_1} t^{n-1} + \frac{W_2}{u_1^2} t^{n-2} + \cdots + \frac{W_n}{u_1^n} = 0$$

und ist demnach auch eine ganze Größe. Die Wiederholung dieser Schlüsse zeigt, daß der Reihe nach auch $\Phi_1, \Phi_2, \ldots$ ganze algebraische Formen sind, die aber ebenso wie Φ_0 die Unbestimmte u_1 nicht mehr enthalten. Der Satz gilt also für Formen von m Unbestimmten, wenn er für Formen von $m-1$ Unbestimmten richtig ist. Da aber für Formen einer Unbestimmten die durchgeführten Schlüsse die Koeffizienten geradezu als ganze algebraische Größen aus Γ ergeben, ist unser Satz in der Tat allgemein gültig.

Die ganzen algebraischen Größen des Gattungsbereichs Γ bilden einen echten holoiden Bereich, den wir mit $[\Gamma]$ bezeichnen; denn er genügt der in Kap. I. § 4 gegebenen Definition und enthält keine Größe erster Ordnung dieses Bereichs, die nicht auch ganz ist. — Ausgenommen ist nur der triviale Fall, wo A ein orthoider Bereich und keine Unbestimmten auftreten. (Siehe diesbezüglich den Schluß von § 4).

Die dem Gattungsbereiche Γ entstammenden ganzen algebraischen Formen sind demnach die dem Bereiche $[\Gamma]$ entstammenden Formen; ihre Gesamtheit bildet einen echten holoiden Bereich, der mit $[\Gamma]_w$ bezeichnet werden soll.

Die primitiven ganzen algebraischen Formen.

§ 4. Der soeben definierte echte holoide Bereich $[\Gamma]$ ist nur in den allereinfachsten Fällen ein vollständiger Bereich. (Siehe die Anmerkung zu § 7.)

Fällt aber der Begriff des größten gemeinschaftlichen Teilers fort, so kann auch die Definition der primitiven Formen in Kap. III. § 9 nicht mehr aufrecht erhalten bleiben. An Stelle derselben tritt nun die folgende*):

Eine dem Bereiche $[\Gamma]$ entstammende Form Φ heißt primitiv (oder eine Einheitsform), wenn Nm. Φ eine primitive Form der Unbestimmten $u_1, \ldots$ ist. Dabei ist — was wieder ein für allemal bemerkt werden soll — Nm. Φ als dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form zu betrachten.

Für die Form Nm. Φ, deren Koeffizienten dem vollständigen holoiden Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehören, bleibt die frühere Definition bestehn.

Daß diese Definition, sobald $[\Gamma]$ ein vollständiger holoider Bereich ist, mit der früheren übereinstimmt, ist unmittelbar einzusehn. Denn Nm. Φ wird in diesem Falle dann und nur dann primitiv sein, wenn dies für die Faktoren $\Phi_1, \Phi_2, \ldots, \Phi_n$ der Fall ist. Dann sind aber $\delta_1, \ldots, \delta_n$ (die größten gemeinschaftlichen Teiler der Koeffizienten von $\Phi_1, \ldots, \Phi_n$) auch konjugierte Größen. Aus $\delta_1 \sim 1$ oder $\delta_1 \varepsilon_1 = 1$ folgt aber auch $\delta_2 \varepsilon_2 = 1$ und $\delta_2 \sim 1$ u. s. f. Von den Größen δ sind also alle, oder keine einzige ~ 1. Andrerseits ist aber der größte gemeinschaftliche Teiler der Koeffizienten von Nm. Φ geradezu

*) Kronecker, Festschrift, § 15.

$\sim \delta_1 \delta_2 \ldots \delta_n$, also im ersten Falle ~ 1 und im zweiten Falle nicht ~ 1, denn aus $\delta_1 \ldots \delta_n \sim 1$ würde, da $\delta_2 \ldots \delta_n$ ganz und auch eine Größe des Bereichs Γ_1 ist, $\delta_1 \sim 1$ folgen.

Für die so erweiterte Definition der primitiven Form gilt, wie unmittelbar zu sehn, der Fundamentalsatz:

Das Produkt primitiver Formen ist wieder eine primitive Form.

Dabei sind immer dem Bereiche $[\Gamma]$ entstammende Formen zu verstehn. Man hat dann noch den weiteren wichtigen Satz*):

Ist Φ eine primitive ganze algebraische Form von $u_1, u_2, \ldots$, Ψ eine beliebige ganze algebraische Form, ferner X eine ganze algebraische Form, welche die Unbestimmten u nicht enthält, so kann $\Phi\Psi$ nur dann durch X teilbar sein, wenn schon Ψ durch X teilbar ist.

Aus der Voraussetzung

$$\Phi\Psi = XH,$$

wo nun auch H eine ganze algebraische Form ist, folgt

$$\Phi(Xz - \Psi) = X(\Phi z - H)$$

und demnach auch

$$\text{Nm. } \Phi \text{ Nm. } (Xz - \Psi) = \text{Nm. } X \text{ Nm. } (\Phi z - H).$$

Dann muß aber, weil Nm. Φ primitiv ist, Nm. $(Xz - \Psi)$ durch Nm. X teilbar sein.

Es ist also

$$\text{Nm.}\left(z - \frac{\Psi}{X}\right)$$

eine Form, deren Koeffizienten dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehören, und es ist darin der Koeffizient von z^n gleich Eins.

Da weiter in Φ nur die Unbestimmten $u_1, u_2, \ldots$ enthalten sind, muß jedenfalls $\frac{H}{\Phi}$ eine Form der in Ψ enthaltenen

*) Kronecker, Festschrift, § 15.

weiteren Unbestimmten $v_1, \ldots$ sein, vorläufig allerdings nur in dem Sinne, daß die Koeffizienten noch den Nenner Φ mit den Unbestimmten u enthalten können. Da aber dieselbe Form resultiert, wenn man nach dem gewöhnlichen Divisionsverfahren $\frac{\Psi}{X} = \frac{H}{\Phi}$ bildet, sieht man, daß die wirklich auftretenden Nenner die Unbestimmten u auch nicht enthalten können. Es ist also $\frac{\Psi}{X}$ jedenfalls eine algebraische Form der u und v, und da sie endlich der Gleichung

$$\text{Nm.}\left(z - \frac{\Psi}{X}\right) = 0$$

genügt, nach den für die linke Seite dieser Gleichung statuierten Eigenschaften auch eine ganze algebraische Form, w. z. b. w.

Die beiden Fälle, wo A einen orthoiden Bereich oder aber den Bereich [1] bedeutet, gestatteten bisher eine völlig gleiche Behandlung. Um, wo dies notwendig scheint, bei der Trennung beider Fälle eine kürzere Ausdrucksweise zu gewinnen, werden wir jene Größen und Formen, bei deren Definition ein orthoider Bereich A zu Grunde liegt, als relativ ganze, (in Bezug auf A ganze) Größen und Formen bezeichnen und im Gegensatze hierzu, wenn $A = [1]$ ist, von absolut ganzen Größen und Formen sprechen.

Selbstverständlich hat, wenn A ein orthoider Bereich ist, nur der Fall ein Interesse, wo Unbestimmte $x_1, x_2, \ldots$ wirklich auftreten; ist $m = 0$, so wird in dem A entstammenden Gattungsbereiche jede Größe ganz zu nennen sein, und die Theorie der ganzen Größen verliert ihren Inhalt.

§ 5. Es seien

$$\alpha_0, \alpha_1, \alpha_2, \ldots$$

irgend welche Größen des Bereichs $[\Gamma]$,

$$U_{k_0}, U_{k_1}, U_{k_2}, \ldots$$

irgend welche verschiedene Potenzprodukte der Unbestimmten $u_1, u_2, \ldots$, also $\sum_{(r)} \alpha_r U_r$ eine dem Bereiche $[\Gamma]$ entstammende ganze algebraische Form, für die wir noch die kurze Bezeichnung α_u einführen. Dann ist Nm. α_u eine dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form der u. In dieser Auffassung ist der größte gemeinschaftliche Teiler der Koeffizienten in Nm. α_u eine Größe des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$, und wenn wir diese Größe mit D bezeichnen, $\frac{\text{Nm. } \alpha_u}{D}$ eine dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende primitive Form, die, in völlig bestimmter Weise aus α_u hergeleitet, als „Form von α_u“*)

$$\text{Fm. } \alpha_u = \frac{\text{Nm. } \alpha_u}{D}$$

bezeichnet werden soll.

Bei der hieraus resultierenden Darstellung von Nm. $\alpha_u = D$ Fm. α_u ergibt sich nun der merkwürdige, für Kroneckers arithmetische Theorie der algebraischen Größen grundlegende Satz, daß nur Fm. α_u von der Wahl der Potenzprodukte U abhängt, während die Größe D für alle irgendwie aus sämtlichen Koeffizienten α aufgebauten Formen im Sinne der Äquivalenz unveränderlich (invariant) ist, d. h. durch den Größenkomplex $(\alpha_0, \alpha_1, \ldots)$ bestimmt wird.

Zum Beweise dieses wichtigen Satzes seien

$$\beta_0, \beta_1, \beta_2, \ldots$$

die Koeffizienten α in irgend einer beliebig geänderten Reihenfolge, ferner

$$V_{i_0}, V_{i_1}, V_{i_2}, \ldots$$

irgend welche wieder verschiedene Potenzprodukte der Unbestimmten $v_1, v_2, \ldots$, wo die v zum Teile oder ganz mit den früher gebrauchten u übereinstimmen, oder von diesen auch

*) Kronecker, Festschrift, § 14.

durchweg verschieden sein können. Aus diesen Größen bilden wir die Form

$$\beta_u = \sum_{(s)} \beta_s V_s .$$

Dann ist nachzuweisen, daß, wenn man wieder

$$\text{Nm. } \beta_v = D' \text{ Fm. } \beta_v$$

setzt, $D' \sim D$ ist.

Es ist, ausführlich geschrieben, gemäß der Definition der Norm

$$\text{Nm. } \beta_v = \prod_{i=1}^{n} \beta_v^{(i)};$$

wählt man nun aus jeder Form $\beta_v^{(i)}$ einen beliebigen Koeffizienten $\beta_{\mu_i}^{(i)}$ und bildet das Produkt

$$\pi_\mu = \beta_{\mu_1}^{(1)} \beta_{\mu_2}^{(2)} \cdots \beta_{\mu_n}^{(n)},$$

wo die Indices $\mu_1, \mu_2, \ldots, \mu_n$ ganz unabhängig voneinander gewählt werden können, so genügt jede Größe π_μ nach dem Kroneckerschen Fundamentalsatze (Kap. III. § 7) einer Identität von der Gestalt:

$$\pi_\mu^\nu + A_1^{(\mu)} \pi_\mu^{\nu-1} + \cdots + A_\nu^{(\mu)} = 0,$$

wo $A_k^{(\mu)}$ eine rationale und ganze homogene Form k^{ter} Dimension der in Nm. β_v auftretenden Koeffizienten ist. Dabei ist Nm. β_v als dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form der v aufzufassen. Den größten gemeinschaftlichen Teiler dieser Koeffizienten haben wir oben mit D' bezeichnet, und es ist demnach $A_k^{(\mu)}$ durch D'^k teilbar. Jene Identität kann aber auch

$$\left(\frac{\pi_\mu}{D'}\right)^\nu + \frac{A_1^{(\mu)}}{D'} \left(\frac{\pi_\mu}{D'}\right)^{\nu-1} + \cdots + \frac{A_\nu^{(\mu)}}{D'^\nu} = 0$$

geschrieben werden und zeigt in dieser Gestalt unmittelbar, daß $\frac{\pi_\mu}{D'}$ eine ganze Größe ist.

Nun ist aber jeder Koeffizient in Nm. α_u, als Form der u, eine Summe von Größen π_μ, also auch durch D' teilbar, und

demnach D' ein Teiler von D, dem größten gemeinschaftlichen Teiler der Koeffizienten von Nm. α_u. Genau dieselben Schlüsse gelten aber auch, wenn man die Rollen der Formen α_u und β_v miteinander vertauscht; es ist also auch D ein Teiler von D' und demnach, wie zu beweisen war*),

$$D \sim D'.$$

§ 6. Die aus der Form α_u hergeleitete primitive Form Fm. α_u besitzt noch weitere wichtige Eigenschaften, die als Vorbereitung für die Theorie der Teilbarkeit in $[\Gamma]$ hier darzulegen sind. Diese sind in den beiden folgenden Sätzen ausgedrückt.

I. Sind α_u und β_v zwei — im früher erörterten Sinne — aus derselben Koeffientenreihe aufgebaute Formen, so ist β_v Fm. α_u in $[\Gamma]_w$ durch α_u teilbar, d. h. es gibt eine dem Bereiche $[\Gamma]$ entstammende ganze algebraische Form γ_w, für die

$$\beta_v \text{ Fm. } \alpha_u = \alpha_u \gamma_w$$

ist.

Man bestimmt nämlich γ_w als ganze algebraische Form einfach durch die Bemerkung, daß

$$\frac{\beta_v \text{ Fm. } \alpha_u}{\alpha_u} = \frac{1}{D} \beta_v \frac{\text{Nm } \alpha_u}{\alpha_u}$$

in der Tat eine ganze Form sein muß. Es ist dieser Quotient, ausführlich geschrieben:

$$\frac{1}{D} \sum_{(s)} \beta_s^{(1)} V_s \prod_{i=2}^{n} \sum \alpha_r^{(i)} U_r,$$

und hierin wird der Koeffizient jedes Potenzproduktes $V_s U_r$

*) Die mehrfach hervorgehobenen Schwierigkeiten, die sich dem Verständnisse des § 14 der Kroneckerschen Festschrift entgegenstellen, werden durch Voranstellung des hier citierten Fundamentalsatzes und den hier selbständig gefaßten Folgesatz desselben in elementarer Weise gehoben. (Siehe die Anmerkungen zu Kap. III. § 4 und 5.)

eine Summe von Größen π_μ (wo die π_μ die in § 5 festgesetzte Bedeutung haben) und ist also in der Tat durch D teilbar.

II. Ist Φ eine beliebige, und E eine primitive Form aus $[\Gamma]_w$, ferner ΦE durch α_u teilbar, so ist auch Φ Fm. α_u durch α_u teilbar.

Die Voraussetzung unsres Satzes wird durch eine Identität

$$\Phi E = \alpha_u \Psi$$

ausgedrückt, wo Ψ eine Form des Bereichs $[\Gamma]_w$ ist.

Ist nun β_v wieder eine aus der Koeffizientenreihe von α_u aufgebaute Form, wo aber nun die v neue, von den in den gegebenen Formen auftretenden Unbestimmten verschiedene Unbestimmte sein sollen, so hat man nach (I.)

$$\alpha_u \text{ Fm. } \beta_v = \beta_v \gamma_w,$$

also

$$\Phi E \text{ Fm. } \beta_v = \Psi \beta_v \gamma_w$$

und, da β_v eine Form ist, die keine der in der primitiven Form E auftretenden Unbestimmten enthält, nach dem am Schlusse von § 4 bewiesenen Satze, auch schon Φ Fm. β_v durch β_v teilbar, d. h.

$$\Phi \text{ Fm. } \beta_v = \beta_v \gamma'_w.$$

Ist $\alpha_{u'}$ jene Form, die aus α_u entsteht, wenn man an Stelle der Unbestimmten $u_1, u_2, \ldots$ wieder die neuen Unbestimmten $u_1', u_2', \ldots$ setzt, so ist nach (I) wieder

$$\beta_v \text{ Fm. } \alpha_{u'} = \alpha_{u'} \gamma''_w,$$

also Φ Fm. β_v Fm. $\alpha_{u'}$ durch $\alpha_{u'}$, oder endlich, da die primitive Form Fm. β_v keine der Unbestimmten u' enthält, wieder nach § 4 auch schon Φ Fm. $\alpha_{u'}$ durch $\alpha_{u'}$ teilbar. Das ist aber der ausgesprochene Satz, in dem nur für die Unbestimmten $u_1, u_2, \ldots$ die Zeichen $u_1', u_2', \ldots$ gesetzt sind.

Die Association der idealen Größen.

§ 7. Die in diesem Kapitel definierten echten holoiden Bereiche $[\Gamma]$ und $[\Gamma]_w$ sind im allgemeinen, d. h. mit Aus-

nahme sehr spezieller Fälle, nicht vollständig*). Es entsteht dadurch eine neue, formell und materiell gleich wichtige Fragestellung, die schon in Kap. III. § 13 gestreift wurde. Der Bereich $[\Gamma]$ soll dergestalt zu einem vollständigen holoiden Bereiche erweitert werden, daß nicht nur die auf die additive und multiplikative Verknüpfung, sondern auch die auf Teilbarkeit bezüglichen Eigenschaften der sämtlichen in $[\Gamma]$ enthaltenen Größen in dem zu bildenden neuen Bereiche erhalten bleiben. Genauer ausgedrückt: Sind $\alpha, \beta, \gamma, \ldots$ irgend welche Größen aus $[\Gamma]$, so soll es in dem neuen erweiterten Bereiche Größen geben, für die man die Symbole $\alpha, \beta, \gamma, \ldots$ so benutzen kann, daß die Beziehungen $\alpha + \beta = \gamma$ oder $\alpha\beta = \gamma$ immer nur in beiden Bereichen zugleich gültig sind, und ebenso immer in beiden Bereichen zugleich α durch β teilbar oder nicht teilbar ist.

Selbstverständlich muß bei diesen Bedingungen auch der erweiterte Bereich ein echter holoider Bereich sein, und die bisher näher untersuchten Fälle einer solchen Erweiterung des Bereichs $[\Gamma]$, der zugeordnete orthoide Bereich (Γ), sowie die diesem entstammenden Gattungsbereiche genügen diesen Forderungen nicht.

---

*) Ist z. B. Γ der aus (1) durch Adjunktion einer Wurzel der Gleichung $x^2 + 5 = 0$ entstandene Gattungsbereich, so sind die Größen dieses Bereichs $r + s\sqrt{-5}$, wo r und s Zahlen aus (1) bedeuten. Soll nun $r + s\sqrt{-5}$ eine absolut ganze Größe sein, so muß auch $r - s\sqrt{-5}$, also ferner $2r$ und $2s\sqrt{-5}$, sowie $20s^2 = 5 \cdot (2s)^2$ und schließlich $2s$ ganz sein. D. h. jene Größe $r + s\sqrt{-5}$ muß die Gestalt $\frac{a + b\sqrt{-5}}{2}$ haben, wo a und b Zahlen aus [1] sind. Dann muß wieder $\frac{a^2 + 5b^2}{4}$ und auch $\frac{a^2 + b^2}{4}$ ganz sein. Dies ist aber nur dann der Fall, wenn a und b gerade sind. In unserem Beispiele ist also der Bereich $[\Gamma]$ der in Kap. I. § 8 mit $[\sqrt{-5}]$ bezeichnete Bereich und, wie dort gezeigt wurde, nicht vollständig.

Die Gesamtheit der Quotienten $\frac{\gamma_u}{\varepsilon_v}$, wo γ_u eine beliebige Form aus $[\Gamma]_w$ und ε_v eine beliebige primitive Form (Einheitsform) desselben Bereichs bedeutet, gibt in einfachster Weise einen Bereich, der den soeben aufgestellten Bedingungen in sämtlichen Stücken genügt. Dabei soll — was wohl natürlich, aber nicht selbstverständlich ist — die Addition und Multiplikation in diesem Bereiche durch

$$\frac{\gamma'_{u'}}{\varepsilon'_{v'}} + \frac{\gamma''_{u''}}{\varepsilon''_{v''}} = \frac{\gamma'_{u'}\varepsilon''_{v''} + \gamma''_{u''}\varepsilon'_{v'}}{\varepsilon'_{v'}\varepsilon''_{v''}}$$

$$\frac{\gamma'_{u'}}{\varepsilon'_{v'}} \cdot \frac{\gamma''_{u''}}{\varepsilon''_{v''}} = \frac{\gamma'_{u'}\gamma''_{u''}}{\varepsilon'_{v'}\varepsilon''_{v''}}$$

definiert sein, also sich genau nach den im orthoiden Bereiche $([\Gamma]_w)$ gültigen Gesetzen vollziehen.

Es sind nun die den aufgestellten Forderungen entsprechenden Eigenschaften des so definierten Bereichs nachzuweisen, der, um uns kurz ausdrücken zu können, mit $[\mathfrak{G}]$ bezeichnet werde. Nach der Definition dieses Bereichs besitzen die ihm angehörenden Größen alle für die Quotienten $\frac{\gamma_u}{\varepsilon_v}$ nach den Regeln der elementaren Algebra bestehenden Eigenschaften und bilden, da das Produkt primitiver Formen wieder eine primitive Form ist, jedenfalls einen holoiden Bereich. Es ist aber auch $[\mathfrak{G}]$ ein echter holoider Bereich, da z. B. die Gleichung $2x = 1$ in $[\mathfrak{G}]$ keine Lösung besitzt. Im entgegengesetzten Falle müßte eine Beziehung $2\gamma_u = \varepsilon_v$ existieren, und das ist unmöglich, da sonst die Norm der primitiven Form ε_v durch 2 teilbar, also nicht primitiv wäre.

Die Einheiten des Bereichs $[\mathfrak{G}]$ sind die Größen von der Gestalt $\frac{\varepsilon'_u}{\varepsilon_v}$, wo auch der Zähler ε'_u eine primitive Form ist. Da auch $\frac{\varepsilon_v}{\varepsilon'_u}$ dem Bereiche $[\mathfrak{G}]$ angehört, sind die so definierten Größen jedenfalls Einheiten; aber auch nur diese, denn es muß, wenn $\frac{\gamma_u}{\varepsilon_v}$ eine Einheit sein soll, eine zweite Größe $\frac{\gamma'_{u'}}{\varepsilon'_{v'}}$ von der Beschaffenheit geben, daß

$$\gamma_u \gamma'_{u'} = \varepsilon_v \varepsilon'_{v'}$$

wird. Daraus folgt aber, daß Nm. γ_u Nm. $\gamma'_{u'}$, also auch Nm. γ_u und endlich γ_u primitiv ist.

Daß der Bereich [𝔊] ein vollständiger holoider Bereich ist, weisen wir einfach in der Weise nach, daß wir für zwei beliebige Größen des Bereichs, $\frac{\alpha'_{u'}}{\varepsilon'_{v'}}$ und $\frac{\alpha''_{u''}}{\varepsilon''_{v''}}$ in der Tat eine solche Größe des Bereichs [𝔊] bilden, die im Sinne der Definition in Kap. I. § 6 ihr größter gemeinschaftliche Teiler ist.

Es seien $\alpha_1', \alpha_2', \ldots$ die Koeffizienten der Form $\alpha'_{u'}$ und ebenso $\alpha_1'', \alpha_2'', \ldots$ die Koeffizienten von $\alpha''_{u''}$. Es bezeichne ferner γ_w eine aus den Koeffizienten von $\alpha'_{u'}$ und $\alpha''_{u''}$ aufgebaute Form, in der aber auch alle diese Koeffizienten wirklich zur Verwendung kommen, d. h.

$$\gamma_w = \sum_{(r)} \alpha_r' W'_{k_r} + \sum_{(s)} \alpha_s' W_{l_s},$$

wo die W' und W'' durchweg verschiedene Potenzprodukte der Unbestimmten $w_1, w_2, \ldots$ bedeuten. Dann ist, wenn man die ursprüngliche Bezeichnung für den größten gemeinschaftlichen Teiler anwendet:

$$\left(\frac{\alpha'_{u'}}{\varepsilon'_{v'}}, \frac{\alpha''_{u''}}{\varepsilon''_{v''}}\right) \sim \gamma_w,$$

wo statt γ_w jede mit γ_w äquivalente Größe $\gamma_w \frac{\varepsilon_{w'}}{\varepsilon_{w''}}$ gesetzt werden kann*).

Aus den Koeffizienten von $\alpha'_{u'}$ und $\alpha''_{u''}$ bilden wir die lineare Form

$$\sum_{(r)} \alpha_r' t_r' + \sum_{(s)} \alpha_s'' t_s''$$

mit den neuen Unbestimmten t', t''; dann ist nach Satz (I.) in § 6

*) Um die Bedeutung des Zeichens $\sim$ nicht zu verrücken, ist dabei noch zu bemerken, daß die in der Parenthese stehenden Größen selbst dann, wenn z. B. $\varepsilon'_{v'} = 1$, nicht etwa als Formen, sondern als einheitliche Zeichen für Größen aus [𝔊] aufzufassen sind.

$$\left(\sum_{(r)} \alpha_r' t_r' + \sum_{(s)} \alpha_s'' t_s''\right) \text{Fm.}\, \gamma_w = \gamma_w \gamma'_{w'},$$

wo $\gamma'_{w'}$ wieder eine Form aus $[\Gamma]_w$ bedeutet. Da die t neue Unbestimmte sind, stehn in dieser Identität rechts und links lineare Formen der t, und man hat, wenn man die Koeffizienten der t vergleicht, für jedes α eine Identität von der Gestalt

$$\alpha\, \text{Fm.}\, \gamma_w = \gamma_w \gamma''_{w''},$$

also geradezu einen Ausdruck der Tatsache, daß α in $[\mathfrak{G}]$ durch γ_w teilbar ist, da ja $\frac{\gamma''_{w''}}{\text{Fm.}\, \gamma_w}$ eine Größe des Bereichs $[\mathfrak{G}]$ ist. Dasselbe ist dann auch für $\alpha'_{u'}$ und $\alpha''_{u''}$ und endlich für die mit ihnen äquivalenten Größen $\frac{\alpha'_{u'}}{\varepsilon'_{v'}}$ und $\frac{\alpha''_{u''}}{\varepsilon''_{v''}}$ der Fall. D. h. γ_w ist jedenfalls ein gemeinschaftlicher Teiler dieser Größen.

Es ist endlich γ_w der gesuchte größte gemeinschaftliche Teiler, wenn jeder Teiler von $\alpha'_{u'}$ und $\alpha''_{u''}$ auch ein Teiler von γ_w ist*). Um dies nachzuweisen, bemerken wir zuerst, daß in Wiederholung der soeben angewandten Schlußweise nach § 6 auch eine Identität

$$\left(\sum_r \alpha_r' t_r'\right) \text{Fm.}\, \alpha'_{u'} = \alpha'_{u'} \beta_v$$

besteht und aus dieser, genau wie früher, folgt, daß jeder Koeffizient α' durch $\alpha'_{u'}$, also auch durch jeden Teiler von $\alpha'_{u'}$ teilbar. Es sind also die Koeffizienten α' und α'' durch jeden gemeinschaftlichen Teiler von $\alpha'_{u'}$ und $\alpha''_{u''}$ teilbar, und dasselbe gilt für die Größe γ_w in $[\mathfrak{G}]$. Damit ist nicht nur bewiesen, daß der Bereich $[\mathfrak{G}]$ ein vollständiger ist, sondern auch ein Verfahren erlangt, den größten gemeinschaftlichen

*) Der Kürze wegen sind hier die im Zähler stehenden Formen statt der mit ihnen äquivalenten Quotienten geschrieben, was, wenn wir nur nicht vergessen, daß die Teilbarkeit in $[\mathfrak{G}]$ zu verstehn ist, an der Richtigkeit oder Allgemeinheit der ausgesprochenen Tatsachen nichts ändert.

Teiler zweier Größen des Bereichs in fertiger Gestalt unmittelbar zu bilden*).

§ 8. Die Größen des Bereichs $[\mathfrak{G}]$ gehören entweder schon dem Bereiche $[\Gamma]$ an, oder sie sind neue, dem Bereiche $[\Gamma]$ associierte Größen, wenn wir unter Association eben eine den jetzt gestellten Bedingungen entsprechende Erweiterung des gegebenen Bereichs verstehen**). (Ähnlich war früher die Adjunktion eine solche Erweiterung eines gegebenen holoiden Bereichs, bei welcher gleichfalls die Regeln für die additive und multiplikative Verknüpfung der ursprünglichen Größen ungeändert bleiben, weiter aber noch eine Reihe von im ursprünglichen Bereiche unlösbaren Gleichungen nun lösbar wird).

Eine Größe, die dem Bereiche $[\mathfrak{G}]$ angehört, soll als ideale Größe des Bereichs $[\Gamma]$ bezeichnet werden; es ist dies eine nicht ganz genaue, aber bequeme Ausdrucksweise, die sich auch in andern mathematischen Disziplinen wiederfindet. (So spricht man z. B. von den imaginären Punkten einer Geraden u. s. f.). Die ideale Größe des Bereichs $[\Gamma]$ im weiteren Sinne des Wortes kann auch eine Größe sein, die die dem Bereiche $[\Gamma]$ „wirklich" angehört; ist dies nicht der Fall, so ist sie eine ideale Größe im engeren Sinne des Wortes.

*) Der Beweis dafür, daß, wenn α und β Größen des Bereichs $[\Gamma]$ sind, α durch β auch in $[\mathfrak{G}]$ nur dann teilbar ist, wenn dies schon in $[\Gamma]$ der Fall war, mag noch in einigen Worten ausgeführt werden. Ist α durch β in $[\mathfrak{G}]$ teilbar, so ist α Fm. β durch β in $[\Gamma]_w$ teilbar; nun ist aber Fm. $\beta = 1$, also muß α durch β in $[\Gamma]_w$ und demnach auch schon in $[\Gamma]$ teilbar sein.

**) Daß die hier associierten Größen „Größen" im vollen Sinne des Wortes sind, d. h. sowohl die Addition, wie die Multiplikation gestatten, und nicht bloß die letztere, wie in Dedekinds Theorie der Ideale und Kroneckers Darstellung, halte ich für einen nicht bloß formalen Fortschritt in der auf die Erhaltung des Divisorenbegriffs abzielenden mathematischen Begriffsbildung. (Siehe hierauf bezüglich die Anmerkung zu § 24.) Damit ist auch die scharfe Grenze zwischen „Teilern" und „Divisorensystemen" gezogen.

Für den speziellen Fall der Theorie der algebraischen Zahlen hat schon H. Weber in seinem „Lehrbuch der Algebra", II. Bd. § 154 solche Größen benutzt, die von ihm s. g. ganzen Funktionale.

Eine nur im Sinne der Äquivalenzbestimmung gegebene ideale Größe des Bereichs $[\Gamma]$ wird nach Dedekind als Ideal bezeichnet. Dabei ist aber zu beachten, daß die Definition des Ideals innerhalb der Dedekindschen Theorie selbst eine gewisse Umwandlung erleidet. Ursprünglich ist in dieser als „Ideal" jede solche Menge von Größen aus $[\Gamma]$ zu verstehn, welche die folgende Eigenschaft besitzt: Sind α und β zwei Größen der Menge, und γ eine beliebige Größe aus $[\Gamma]$, so gehören auch $\alpha + \beta$ und $\alpha\gamma$ zur Menge. Sind nun $(\alpha_1, \alpha_2, \ldots)$ und $(\beta_1, \beta_2, \ldots)$ zwei solche Mengen oder Ideale, so ist auch die aus allen Produkten der Gestalt $\alpha_i\beta_j$ und allen Summen solcher Produkte bestehende Menge ein „Ideal". Diese „Multiplikation der Ideale" ist nichts anderes, als das, was wir früher (Kap. VII) als Komposition zweier Divisorensysteme bezeichnet haben, wenn wir diese Ideale als Divisorensysteme „mit unendlich vielen Elementen" auffassen. Dedekinds „höchst sorgfältige und scharfsinnige Art der Deduktion, die bei seinen ganz abstrakten Begriffsbestimmungen ebenso notwendig, als bewundernswert erscheint"*) fährt dann folgendermaßen fort. Es wird einerseits bewiesen, daß jedes so aufgefaßte Ideal einem Divisorensystem mit einer endlichen Anzahl von Elementen äquivalent ist, anderseits, daß, wenn ein solches Divisorensystem oder Ideal $(\alpha_1, \alpha_2, \ldots)$ ein zweites $(\beta_1, \beta_2, \ldots)$ enthält, es immer auch als Produkt aus $(\beta_1, \beta_2, \ldots)$ und einem dritten Ideal dargestellt werden kann**). Faßt man endlich das Ideal nicht mehr als Größenmenge, sondern als durch eine

*) Kroneckers Worte in der Festschrift am Ende des § 21.

**) Allerdings ist dieser Beweis nur für den Fall der algebraischen Zahlen und der algebraischen Funktionen einer Veränderlichen durchgeführt (siehe das Citat in § 1), und es muß dahingestellt bleiben, welche Schwierigkeiten sich dem Beweise im allgemeinen Falle der absolut ganzen Größen entgegenstellen würden, wenn man ausschließlich nur die nach Dedekind gestatteten Hilfsmittel benutzen darf. Die von verschiedenen Autoren für die Dedekindsche Idealtheorie gegebenen „Vereinfachungen" beruhen durchweg auf einer mehr oder weniger verhüllten Anwendung der Kroneckerschen Grundideen.

endliche Anzahl von Größen aus $[\Gamma]$ definiertes Symbol, für das die früher angedeutete Multiplikationsregel besteht, so bildet die Gesamtheit dieser Symbole einen Bereich, für den zwar kein Additionsgesetz, wohl aber das gewöhnliche Multiplikationsgesetz besteht, und der — wie man leicht zeigt — insofern ein vollständiger ist, als der größte gemeinschaftliche Teiler zweier Ideale wieder ein Ideal ist. Ist endlich α eine bestimmte, μ eine beliebige Größe aus $[\Gamma]$, so kann das aus allen Produkten $\alpha\mu$ hergeleitete Ideal als Symbol durch α bezeichnet werden, und diese Symbole α stimmen mit den Größen α in allen auf die Multiplikation und Teilbarkeit bezüglichen Eigenschaften überein. Es ist aber dann das gestellte Problem, allerdings mit der Beschränkung auf nur multiplikativ verwendbare Größen gelöst, und man kann nun in der Tat das Ideal als eine nur durch Äquivalenzbestimmung gegebene ideale Größe des Bereichs $[\Gamma]$ betrachten*). Es wird demgemäß nach Grundlegung der Theorie — auch bei Benutzung der einschlägigen Literatur — gleichgültig sein, ob wir das Ideal in der einen oder andern Weise definieren wollen. In jenen Fällen nämlich, wo die Dedekindsche Theorie der Ideale nicht ausgeführt ist, kann man nach den bisherigen Entwicklungen unmittelbar erkennen, daß die Gesamtheit der Größen aus $[\Gamma]$, die durch eine bestimmte Größe aus $[\mathfrak{G}]$ teilbar sind, ein Ideal im Sinne Dedekinds bilden, und daß dieses Ideal, soweit nur Äquivalenzbestimmungen in Betracht kommen, jene Größe aus $[\mathfrak{G}]$ vollständig vertritt.

Kronecker bezeichnet die nur durch Äquivalenzbestimmung gegebenen idealen Größen als algebraische Divisoren, ein Ausdruck, der in der Anwendung vielfach unbequem ist und wohl auch deshalb in der Literatur wenig benutzt wird. Wenn auch wir in diesem Falle von der Kroneckerschen Terminologie abweichen, so geschieht dies nicht nur aus

*) Auf die Kummersche Auffassung der idealen Zahl, die von unvergänglicher, aber heute doch nur mehr historischer Bedeutung ist, soll eben deshalb hier nicht eingegangen werden.

den eben angeführten Gründen, sondern auch in Berücksichtigung der historischen Entwicklung, sowie der evidenten Analogie bei Einführung der imaginären und der idealen Größen.

Um durch eine zweckmäßige Bezeichnung die Darstellung übersichtlicher zu gestalten, sollen die idealen Größen des Bereichs $[\Gamma]$ im weiteren Sinne des Wortes, d. h. beliebige Größen aus $[\mathfrak{G}]$ durch kleine gotische Buchstaben, $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ bezeichnet werden. Für die Größen, die im engeren Sinne des Wortes, d. h. „wirklich" dem Bereiche $[\Gamma]$ angehören, bleiben die kleinen griechischen Buchstaben $\alpha, \beta, \gamma, \ldots$ vorbehalten.

§ 9. Wenn die bei Bildung einer idealen Größe des Bereichs $[\Gamma]$:

$$\mathfrak{a} = \frac{\Sigma \alpha_r U_r}{\Sigma \varepsilon_s V_s}$$

zur Verwendung gelangenden Größen α, ε durchweg dem Formenbereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehören, d. h. ganze algebraische Größen erster Ordnung des Gattungsbereichs (Γ) sind, wird es angezeigt sein, auch diese kurz als (in Bezug auf $[\mathsf{A}, x_1, \ldots, x_m]$) rational und ganz zu bezeichnen.

Die Norm einer beliebigen idealen Größe $\mathfrak{a}$ des Bereichs $[\Gamma]$ wird nach dem früheren durch

$$\text{Nm. } \mathfrak{a} = \prod_{i=1}^{n} \frac{\Sigma \alpha_r^{(i)} U_r}{\Sigma \varepsilon_s^{(i)} V_s}$$

definiert, ist demnach immer rational, d. h. ein Quotient zweier Formen aus $[\mathsf{A}, x_1, \ldots, x_m, u_1, \ldots, v_1, \ldots]$, wo der Nenner jedenfalls primitiv, also auch eine Größe aus $[\mathfrak{G}]$ ist; in diesem Sinne ist also Nm. $\mathfrak{a}$ immer rational und ganz.

Zur Grundlegung der hier entwickelten allgemeinen Theorie des größten gemeinschaftlichen Teilers sind noch folgende Bemerkungen hinzuzufügen.

Sind

$$\mathfrak{a} = \frac{\alpha_u}{\varepsilon'_{w'}}, \quad \mathfrak{b} = \frac{\beta_v}{\varepsilon''_{w''}}$$

zwei ideale Größen des Bereichs $[\Gamma]$, so können die in ihnen

auftretenden Koeffizienten in verschiedenster Weise als gewissen Gattungsbereichen angehörend betrachtet werden. Dabei ist es aber möglich, die in

$$\mathfrak{d} \sim (\mathfrak{a}, \mathfrak{b})$$

gegebene Definition des größten gemeinschaftlichen Teilers von der Wahl dieses Gattungsbereichs ganz unabhängig zu gestalten; denn wir können unter den äquivalenten Größen jene wählen, in denen der Nenner gleich Eins ist.

Insbesondere ist die durch

$$(\mathfrak{a}, \mathfrak{b}) \sim 1$$

ausgedrückte Eigenschaft der idealen Größen $\mathfrak{a}$ und $\mathfrak{b}$ unabhängig von der Wahl des Gattungsbereichs Γ, wenn dieser nur die Koeffizienten α, β enthält.

Seien (Γ_1) und (Γ_2) zwei solche Gattungsbereiche und (Γ_3) ein Gattungsbereich, der (Γ_1) und (Γ_2) enthält. Nun ist, wenn nur β_v so geschrieben wurde, daß die in β_v auftretenden Potenzprodukte V von den in α_u benutzten Potenzprodukten U durchweg verschieden sind,

$$\mathfrak{d} \sim \alpha_u + \beta_v$$

und also

$$\text{Nm. } \mathfrak{d} \sim \text{Nm. } (\alpha_u + \beta_v).$$

Dabei hat aber Nm. $(\alpha_u + \beta_v)$ eine verschiedene Bedeutung, je nachdem (Γ_1), (Γ_2) oder (Γ_3) zu Grunde gelegt wird. Sei Nm. $(\alpha_u + \beta_v)$ in diesen drei Fällen N_1, N_2 und N_3. Dann muß aber

$$N_3 = N_1^{k_1} = N_2^{k_2}$$

sein, und die drei Formen N_1, N_2, N_3 sind demnach zu gleicher Zeit primitiv. Das bedeutet aber geradezu, daß die Äquivalenz $\mathfrak{d} \sim 1$ für die beiden bis auf die festgestellte Bedingung beliebig gewählten Gattungsbereiche Γ_1 und Γ_2 immer zugleich richtig oder falsch ist, w. z. b. w.

Von diesen Betrachtungen ausgehend, gelangt man noch zu folgendem Satze:

Seien α, β und δ „wirkliche“ ganze algebraische Größen eines solchen Gattungsbereichs, dessen „wirkliche“ ganze Größen schon für sich einen vollständigen Bereich bilden, und $\delta \sim (\alpha, \beta)$, so wird auch, für jeden anderen Gattungsbereich (Γ), der α, β und δ enthält, $\delta \sim (\alpha, \beta)$ sein, wenn man zu dem entsprechenden erweiterten Bereiche $[\mathfrak{G}]$ übergeht.

Man hat dann jedenfalls $\alpha = \delta\mu$, $\beta = \delta\nu$, wo auch μ und ν jenem Gattungsbereiche angehören, und für diesen $(\mu, \nu) \sim 1$. Es ist also (μ, ν) auch für jeden der betrachteten Gattungsbereiche ~ 1, woraus in der Tat nach Kap. I. § 6 und dem früher Bewiesenen $(\alpha, \beta) \sim (\delta\mu, \delta\nu) \sim \delta(\mu, \nu) \sim \delta$ folgt.

Besonders wichtig wird der Satz, wenn man α, β in dem Gattungsbereiche erster Ordnung, der in jedem aus $(\mathsf{A}, x_1, \ldots, x_m)$ entstammenden Gattungsbereiche enthalten ist, d. h. in $[\mathsf{A}, x_1, \ldots, x_m]$ selbst wählt, wo dann α, β und auch δ Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ sind. Er lautet in diesem Falle:

Sind a_x und b_x zwei Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$, und d_x ihr größter gemeinschaftlicher Teiler in diesem vollständigen Bereiche, so ist auch beim Übergange von irgend einem aus $(\mathsf{A}, x_1, \ldots, x_m)$ entstammenden Gattungsbereiche (Γ) zu $[\mathfrak{G}]$ für diesen Bereich $d_x \sim (a_x, b_x)$.

Teilbarkeitstheorie der Ideale.

§ 10. Aus dem vollständigen holoiden Bereiche $[\mathfrak{G}]$ entsteht in bekannter Weise der zugeordnete orthoide Bereich $(\mathfrak{G})$, der, wie unmittelbar zu sehn, mit dem $[\Gamma]_w$ zugeordneten orthoiden Bereiche $([\Gamma])_w$ übereinstimmt. Es wird oft bequem sein, $(\mathfrak{G})$ als „vollständigen“ Gattungsbereich und dem gegenüber (Γ) als Gattungsbereich kurzweg oder auch, wo dies zur Klarheit notwendig erscheint, als „wirklichen“ Gattungsbereich zu bezeichnen.

Der Bereich $(\mathfrak{G})$ enthält den vollständigen holoiden Bereich $[\mathfrak{G}]$. Alle Größen von $(\mathfrak{G})$ sind „ideale Größen des Gattungsbereichs (Γ)“, und zwar „ganze ideale Größen“, wenn sie schon dem Bereiche $[\mathfrak{G}]$ angehören; „gebrochene ideale Größen“ im entgegengesetzten Falle. Diese werden zwar hier nicht mehr zur Anwendung gelangen, sind aber bei Weiterführung der Theorie der algebraischen Größen kaum zu vermeiden. Sie können immer so geschrieben werden, daß der Nenner rational und ganz wird.

Die idealen Größen des Gattungsbereichs (Γ), sowohl die ganzen, wie die gebrochenen, können wieder ideale Größen im engeren Sinne des Wortes oder wirkliche Größen des Gattungsbereichs (Γ) sein. Im zweiten Falle sind sie Größen des „wirklichen“ Gattungsbereichs (Γ), im ersten Falle findet dies nicht statt.

Wir werden uns nun mit den auf die Teilbarkeit bezüglichen Eigenschaften der ganzen idealen Größen beschäftigen und, da wir uns dabei durchweg auf die Größen eines Bereichs $[\mathfrak{G}]$ beschränken, die diesbezügliche Aussage weglassen können.

Für die Größen des Bereichs $[\mathfrak{G}]$ hat man in erster Reihe die in Kap. I. § 5 für beliebige holoide Bereiche festgesetzten, auf die Teilbarkeit bezüglichen Definitionen und Sätze. Insbesondere ist eine solche Größe $\mathfrak{p}$ irreduzibel, wenn sie keinen im Sinne der Äquivalenzbestimmung von 1 und $\mathfrak{p}$ verschiedenen Teiler besitzt. Jede echte irreduzible ganze ideale Größe ist aber auch eine Primgröße, weil der Bereich $[\mathfrak{G}]$ ein vollständiger holoider Bereich ist (Kap. I. § 6). Aber auch jede solche Primgröße ist eine irreduzible ganze ideale Größe, und wir werden von nun ab meist die kürzere Bezeichnung benutzen. Als Primgröße hat $\mathfrak{p}$ bekanntlich die fundamentale Eigenschaft, daß ein Produkt zweier ganzer Größen $\mathfrak{a}\mathfrak{b}$ nur dann durch $\mathfrak{p}$ teilbar ist, wenn schon $\mathfrak{a}$ oder $\mathfrak{b}$ den Teiler $\mathfrak{p}$ besitzt.

Man hat nun vor allem auch ein wohldefiniertes Verfahren, um, wenn $\mathfrak{a}$ und $\mathfrak{b}$ zwei ganze ideale Größen sind, zu entscheiden, ob $\mathfrak{a}$ durch $\mathfrak{b}$ teilbar ist.

Dabei können vor allem für $\mathfrak{a}$ und $\mathfrak{b}$ die mit ihnen äquivalenten Formen α_u und β_v gesetzt werden. Es ist also $\mathfrak{b}$ dann und nur dann ein Teiler von $\mathfrak{a}$, wenn α_u durch β_v oder auch $\frac{\beta_v}{\text{Fm.}\,\beta_v}$ teilbar ist. Nun ist aber $\frac{\alpha_u\,\text{Fm.}\,\beta_v}{\beta_v}$ jedenfalls eine Form der u und v und also jedenfalls eine ganze ideale Größe, wenn sie eine ganze algebraische Form ist, d. h. ganze algebraische Koeffizienten hat, was nach den in § 2 auseinandergesetzten Methoden entschieden wird. In diesem Falle ist also $\mathfrak{a}$ durch $\mathfrak{b}$ teilbar, aber auch nur in diesem Falle. Ist nämlich $\alpha_u\,\text{Fm.}\,\beta_v$ im Formenbereiche $[\Gamma]_w$ durch β_v nicht teilbar, so kann auch $\frac{\alpha_u\,\text{Fm.}\,\beta_v}{\beta_v}$ keine ganze ideale Größe sein, d. h. nicht dem Bereiche $[\mathfrak{G}]$ angehören. Sonst gäbe es zwei primitive Formen $\varepsilon'_{u'}$, $\varepsilon''_{u''}$ von der Beschaffenheit, daß

$$\frac{\alpha_u\,\varepsilon'_{u'}\,\text{Fm.}\,\beta_v}{\beta_u\,\varepsilon''_{u''}}$$

eine ganze algebraische Form ist. Dann muß aber nach (II) in § 6, da auch $\varepsilon'_{u'}\,\text{Fm.}\,\beta_v$ eine primitive Form ist, mit $\alpha_u\varepsilon'_{u'}\,\text{Fm.}\,\beta_v$ zugleich schon $\alpha_u\,\text{Fm.}\,\beta_v$ in $[\Gamma]_w$ durch β_v teilbar sein, was das Gegenteil der jetzt getroffenen Annahme besagt.

Man sieht ferner unmittelbar, daß $\mathfrak{b}$ dann und nur dann ~ 1, wenn für die mit $\mathfrak{b}$ äquivalente Form β_v die rationale und ganze Form $\text{Nm.}\,\beta_v$ (als dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form aufgefaßt) primitiv ist.

Um zu entscheiden, ob $\mathfrak{b}$ ein echter Teiler von $\mathfrak{a}$ ist, haben wir noch den folgenden einfachen Satz:

Der Teiler $\mathfrak{b}$ von $\mathfrak{a}$ ist dann und nur dann ein echter Teiler von $\mathfrak{a}$, wenn $\text{Nm.}\,\mathfrak{b}$ ein echter Teiler von $\text{Nm.}\,\mathfrak{a}$ ist.

Ist nämlich $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, so hat man auch $\text{Nm.}\,\mathfrak{a} = \text{Nm.}\,\mathfrak{b}\,\text{Nm.}\,\mathfrak{c}$, und es ist $\mathfrak{b}$ oder $\mathfrak{c}$ dann und nur dann ~ 1, wenn $\text{Nm.}\,\mathfrak{b}$ oder $\text{Nm.}\,\mathfrak{c} \sim 1$ ist. Dieser so einfache Satz wird dadurch wichtig, daß er die Entscheidung über die vorliegende Frage auf den Bereich $[\mathsf{A}, x_1, \ldots, x_m]$ zurückführt. Es ist

$$\text{Nm. } \mathfrak{a} = \frac{\bar{A}\varepsilon_1}{\varepsilon}, \quad \text{Nm. } \mathfrak{b} = \frac{\bar{B}\varepsilon_2}{\varepsilon}, \quad \text{Nm. } \mathfrak{c} = \frac{\bar{C}\varepsilon_3}{\varepsilon},$$

wo $\bar{A}$, $\bar{B}$, $\bar{C}$ Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$, und ε, ε_1, ε_2, ε_3 diesem Bereiche entstammende primitive Formen sind. Es ist also weiter $\mathfrak{b}$ oder $\mathfrak{c}$ dann und nur dann ~ 1, wenn in Bezug auf diesen Bereich $\bar{B}$ oder $\bar{C} \sim 1$; d. h. $\mathfrak{b}$ ein echter Teiler von $\mathfrak{a}$, wenn die Form $\bar{B}$ ein echter Teiler der Form $\bar{A}$ ist.

Man sieht auch, daß die Norm jeder ganzen idealen Größe einer rationalen und ganzen wirklichen Größe aus $[\mathfrak{G}]$, d. h. einer Form aus $[\mathsf{A}, x_1, \ldots, x_m]$ äquivalent ist, was wir des häufigen Gebrauchs wegen besonders erwähnen.

§ 11. Nach Association der idealen Größen eines Gattungsbereichs werden die Gesetze der Teilbarkeit für die ganzen Größen des Bereichs ebenso einfach uud klar, wie im Bereiche der rationalen und ganzen Zahlen. Insbesondere gilt — und darauf beruht eben die Wichtigkeit und Fruchtbarkeit der eingeführten Methoden — der Fundamentalsatz:

Jede ganze ideale Größe des Gattungsbereichs, mit Ausnahme der 0 und der Einheiten, ist als Produkt einer endlichen Anzahl von Primgrößen darstellbar, und zwar ist diese Darstellung im Sinne der Äquivalenz eindeutig bestimmt.

Ist $\mathfrak{a}$ eine solche ganze ideale Größe, die also weder $= 0$, noch ~ 1, so ist ist sie entweder eine Primgröße, oder sie besitzt einen echten Teiler $\mathfrak{b}$. Dann ist aber $\mathfrak{b}$ wieder nicht $= 0$ und auch nicht ~ 1; es ist also $\mathfrak{b}$ entweder eine Primgröße, oder sie besitzt einen echten Teiler $\mathfrak{c}$ u. s. f. In dieser Reihe $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ muß man aber nach einer endlichen Anzahl von Schritten zu einer Primgröße gelangen, die ein Teiler von $\mathfrak{a}$ ist. Denn es ist auch in der Größenreihe Nm. $\mathfrak{a}$, Nm. $\mathfrak{b}$, Nm. $\mathfrak{c}$, ... jede ein echter Teiler der ihr vorangehenden, und dasselbe ist auch für die Reihe $\bar{A}, \bar{B}, \bar{C}, \ldots$ der Fall, wenn diese Größen die den Normen äquivalenten

Formen aus $[A, x_1, \ldots, x_m]$ bedeuten, und die Teilbarkeit auf diesen Bereich bezogen wird. Da nun aber die Form A nur eine endliche Anzahl von echten Teilern besitzt, muß man, wenn die Reihe $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{r}$, ... nicht schon früher abbricht, nach einer endlichen Anzahl von Schritten zu einer Größe $\mathfrak{y}$ gelangen, deren Norm einer irreduzibeln Form $\overline{H}$ aus $[A, x_1, \ldots, x_m]$ äquivalent ist. Diese Größe $\mathfrak{y}$ muß aber dann nach dem letzten Satze in § 10 eine Primgröße sein.

Die mit $\mathfrak{a}$ bezeichnete Größe ist also jedenfalls durch eine Primgröße $\mathfrak{p}_1$ teilbar; dann ist $\mathfrak{a}$ entweder selbst eine Primgröße, die $\sim \mathfrak{p}_1$, oder aber $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{a}_1$, und $\mathfrak{a}_1$ weder 0, noch ~ 1; dann ist wieder $\mathfrak{a}_1$ durch eine Primgröße $\mathfrak{p}_2$ teilbar u. s. f. In der so entstehenden Reihe $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2, \ldots$ ist wieder jede Größe ein echter Teiler der ihr vorangehenden, und die Reihe muß also wieder im Endlichen abbrechen. Man erhält demnach:

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_\varrho ,$$

wo $\mathfrak{p}_1, \ldots, \mathfrak{p}_\varrho$ gleiche oder verschiedene Primgrößen bedeuten, oder, wenn man die äquivalenten Primgrößen vereinigt, auch

$$\mathfrak{a} \sim \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \ldots \mathfrak{p}_r^{a_r} .$$

Daß es keine im Sinne der Äquivalenz von dieser verschiedene Darstellung

$$\mathfrak{a} \sim \mathfrak{q}_1^{b_1} \mathfrak{q}_2^{b_2}, \ldots, \mathfrak{q}_s^{b_s}$$

gibt, folgt in bekannter Weise (siehe z. B. Kap. IV. § 2). Ebenso ersieht man, daß jede von 0 verschiedene Größe $\mathfrak{a}$ nur eine endliche Anzahl nicht äquivalenter Teiler besitzt, die sämtlich in der Gestalt

$$\mathfrak{d} \sim \mathfrak{p}_1^{c_1} \mathfrak{p}_2^{c_2} \ldots \mathfrak{p}_r^{c_r} \qquad (c_h = 0, 1, \ldots, a_h)$$

geschrieben werden können.

Der soeben entwickelte Gedankengang bietet allerdings bloß einen Existenzbeweis der behaupteten Darstellung und ist daher völlig unbrauchbar, wenn wir in weiteren Untersuchungen diese Darstellung als bekannt voraussetzen müssen.

Um diese Lücke auszufüllen, ist noch eine Reihe weiterer Entwicklungen notwendig, und die wirkliche Darstellung von $\mathfrak{a}$ als Produkt von Primgrößen durch ein bestimmtes endliches Verfahren wird demgemäß erst später (§ 26) gegeben werden können.

§ 12. Die Theorie der Teilbarkeit in [1], oder auch allgemeiner in $[\mathsf{A}, x_1, \ldots, x_m]$ einerseits und $[\mathfrak{G}]$ andrerseits unterscheidet sich — trotz des soeben gegebenen gemeinsamen Fundamentalsatzes — sehr wesentlich durch das Auftreten solcher ganzer Größen in $[\mathfrak{G}]$, die nicht rational sind. Dies geschieht, sobald (Γ) nicht mit $(\mathsf{A}, x_1, \ldots, x_m)$ zusammenfällt, also ein eigentlicher Gattungsbereich (d. h. von höherer als der ersten Ordnung) ist. Die hierauf bezüglichen Hauptsätze sind nun aufzuzählen.

I. Jeder ganzen idealen Größe $\mathfrak{a}$ entspricht eine Form A des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$, so daß eine Form dieses Bereichs, als Größe aus $[\mathfrak{G}]$ aufgefaßt, dann und nur dann durch $\mathfrak{a}$ teilbar ist, wenn sie durch A teilbar ist, wo die letztere Teilbarkeit im Formenbereiche $[\mathsf{A}, x_1, \ldots, x_m]$ zu verstehen ist.

Es ist jedenfalls Nm. $\mathfrak{a}$ und auch die mit Nm. $\mathfrak{a}$ äquivalente Form $\bar{A}$ aus $[\mathsf{A}, x_1, \ldots, x_m]$ durch $\mathfrak{a}$ teilbar, also auch jede durch $\bar{A}$ teilbare Form dieses Bereichs. Ist dasselbe auch für eine durch $\bar{A}$ nicht teilbare Form B der Fall, so muß auch der im Formenbereiche gebildete größte gemeinschaftliche Teiler A_1 von $\bar{A}$ und B (nach dem Satze am Ende von § 9) durch $\mathfrak{a}$ teilbar sein. Ist nun wieder B_1 wohl durch $\mathfrak{a}$, nicht aber durch A_1 teilbar, so wird der größte gemeinschaftliche Teiler A_2 von A_1 und B_1 wieder durch $\mathfrak{a}$ teilbar sein u. s. f. In der Formenreihe $\bar{A}, A_1, A_2, \ldots$ ist aber A_r ein Teiler von A_{r-1} und niemals $A_r \sim A_{r-1}$; denn es ist A_r der größte gemeinschaftliche Teiler von A_{r-1} und einer nicht durch A_{r-1} teilbaren Form B_{r-1}; demnach ist $A_r \sim 1$, oder ein echter Teiler von A_{r-1}. Die Reihe muß also in der Weise abbrechen, daß ein Glied ~ 1 wird, oder aber keine durch A_s

nicht teilbare Form B_s existiert, die durch $\mathfrak{a}$ teilbar ist. Man gelangt dadurch in der Tat zu einer Form A, die dann und nur dann ~ 1 sein kann, wenn $\mathfrak{a} \sim 1$ ist.

II. Die einer Primgröße $\mathfrak{p}$ in der angegebenen Weise entsprechende Form P ist eine Primform, und die Nm. $\mathfrak{p}$ äquivalente Form $\overline{P} \sim P^k$. Wäre nämlich $P = P_1 P_2$, so müßte eben, weil $\mathfrak{p}$ eine Primgröße ist, schon P_1 oder P_2 durch $\mathfrak{p}$ teilbar, also nach der für P statuierten Eigenschaft P_1 oder $P_2 \sim 1$ sein.

Nun ist weiter $P = \mathfrak{p}\mathfrak{a}$, mithin

$$\text{Nm. } P = P^n = \text{Nm. } \mathfrak{p} \,.\, \text{Nm. } \mathfrak{a},$$

also $\overline{P} \sim \text{Nm. } \mathfrak{p}$ ein Teiler von P^n und nicht 1, demnach

$$\sim P^k, \; (k = 1, \ldots, n).$$

Man nennt $\mathfrak{p}$ eine Primgröße (Primideal) k^{ten} Grades, wenn Nm. $\mathfrak{p} \sim P^k$ ist.

Die verschiedenen in einer Primform als Teiler enthaltenen Primideale heißen nach Kronecker verbundene Primideale.

III. Ist der der Untersuchung zu Grunde liegende Gattungsbereich (Γ) ein Galoisscher Bereich, so enthält jede rationale und ganze Größe des Bereichs $[\mathfrak{G}]$ jeden ihrer verbundenen Primteiler gleich oft. Da irreduzible Formen aus $[\mathsf{A}, x_1, \ldots, x_m]$, die nicht äquivalent sind, auch in $[\mathfrak{G}]$ relativ prim sind, ist der Satz nur für irreduzible Formen zu beweisen. Es sei für eine solche:

$$P \sim \mathfrak{p}^a \mathfrak{q}^b \mathfrak{r}^c \ldots;$$

dann gilt diese Zerlegung in jedem der konjugierten Bereiche. Wenn man also die n konjugierten Werte von $\mathfrak{p}$ mit $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ bezeichnet und so fort, so hat man auch

$$P \sim \mathfrak{p}_i^a \mathfrak{q}_i^b \mathfrak{r}_i^c \ldots, \quad (i = 1, \ldots, n).$$

Da aber die konjugierten Gattungsbereiche jetzt zusammenfallen, können diese Darstellungen nicht verschieden sein, und man ersieht zuerst unmittelbar, daß konjugierte Primgrößen

jetzt auch verbunden sind; aber auch das Umgekehrte ist richtig. Verbundene Primgrößen sind jetzt immer auch konjugiert. Denn es ist z. B. Nm. $\mathfrak{p}_i$ durch P, also auch durch $\mathfrak{q}_i$ teilbar, und dies findet nur dann statt, wenn irgend ein $\mathfrak{p}_j \sim \mathfrak{q}_i$ ist. Wäre nun z. B. $a < b$, so hätte man, da einer der konjugierten Werte von $\mathfrak{q}_i$, z. B. $\mathfrak{q}_j \sim \mathfrak{p}_i$ sein muß, auch

$$P \sim \mathfrak{p}_j^a \mathfrak{q}_j^b \ldots,$$

d. h. P müßte den Teiler $\mathfrak{p}_i^b$ enthalten. Ebenso wenig kann $b < a$ sein.

Es ist also, wenn $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, ... die in P als Teiler enthaltenen Primgrößen sind,

$$P \sim (\mathfrak{p}\,\mathfrak{q}\,\mathfrak{r} \ldots)^a.$$

§ 13. Ein Ideal, das einer wirklichen Größe des Bereichs $[\Gamma]$ äquivalent ist, wird nach Dedekind ein Hauptideal genannt.

Man erkennt dann sehr leicht die folgende Tatsache:

Ist $\mathfrak{a}$ ein beliebiges Ideal, $\mathfrak{p}$ ein beliebiges Primideal, so gibt es immer ein Hauptideal, das wohl durch $\mathfrak{a}$, aber nicht durch $\mathfrak{a}\mathfrak{p}$ teilbar ist.

Man findet es unmittelbar aus den Koeffizienten der mit $\mathfrak{a}$ äquivalenten Form α_u. Diese Koeffizienten müssen sämtlich durch $\mathfrak{a}$, aber wenigstens einer durch $\mathfrak{a}\mathfrak{p}$ nicht teilbar sein. Im entgegengesetzten Falle wäre ja auch $\mathfrak{a}$ durch $\mathfrak{a}\mathfrak{p}$ teilbar, was unmöglich. Dieser so bestimmte Koeffizient bestimmt im Sinne der Äquivalenz das gesuchte Hauptideal.

Hieraus folgt auch allgemeiner: Ist $\mathfrak{a}$ ein beliebiges Ideal, während $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ beliebige Primideale sind, so gibt es immer ein Hauptideal, das wohl durch $\mathfrak{a}$, aber durch keines der Ideale $\mathfrak{a}\mathfrak{p}_1, \mathfrak{a}\mathfrak{p}_2, \ldots, \mathfrak{a}\mathfrak{p}_r$ teilbar ist.

Es sei $\mathfrak{m}_i$ das Produkt von $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ mit Ausschluß von $\mathfrak{p}_i$. Dann gibt es, wie eben gezeigt wurde, eine wirkliche Größe β_i in $[\Gamma]$, die wohl durch $\mathfrak{a}\mathfrak{m}_i$, aber nicht durch $\mathfrak{a}\mathfrak{m}_i\mathfrak{p}_i$ teilbar ist; und das durch

$$\beta_1 + \beta_2 + \cdots + \beta_r$$

bestimmte Hauptideal besitzt die gesuchte Eigenschaft. Es ist jedenfalls durch $\mathfrak{a}$ teilbar; sollte es auch durch $\mathfrak{a}\mathfrak{p}_i$ teilbar sein, so müßte, da dies gewiß für jedes β mit Ausschluß von β_i stattfindet, auch β_i durch $\mathfrak{a}\mathfrak{p}_i$ teilbar sein. Nun enthält aber $\mathfrak{a}\mathfrak{m}_i\mathfrak{p}_i$ jede Primgröße mit Ausnahme von $\mathfrak{p}_i$ ebenso oft als Teiler wie $\mathfrak{a}\mathfrak{m}_i$, die Primgröße $\mathfrak{p}_i$ aber ebenso oft wie $\mathfrak{a}\mathfrak{p}_i$; es müßte also im Gegensatz zur Annahme β_i durch $\mathfrak{a}\mathfrak{m}_i\mathfrak{p}_i$ teilbar sein.

Man erkennt ferner, daß es unendlich viele (im Sinne der Äquivalenz) verschiedene Hauptideale gibt, die der gestellten Bedingung genügen. Wenn wir z. B. die durch die wirklichen Größen

$$\alpha_1, \alpha_2, \ldots, \alpha_s$$

bestimmten Hauptideale der Aufgabe gemäß bestimmt haben, und nun z. B. $\mathfrak{q}$ ein Primideal ist, das zu $\alpha_1, \alpha_2, \ldots, \alpha_s, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ relativ prim ist, so läßt sich ein Hauptideal α_{s+1} bestimmen, das wohl durch $\mathfrak{a}\mathfrak{q}$, aber durch keine der Größen $\mathfrak{a}\mathfrak{q}\mathfrak{p}_1, \ldots, \mathfrak{a}\mathfrak{q}\mathfrak{p}_r$ teilbar ist, also offenbar wieder die Aufgabe löst und von $\alpha_1, \ldots, \alpha_s$ verschieden ist. Daß man so eine unbegrenzte Reihe von Größen α erhält, ist evident; denn es gibt unendlich viele irreduzible Formen in $[\mathsf{A}, x_1, \ldots, x_m]$, also auch unendlich viele Primideale.

Damit gelangen wir schließlich zu dem schönen, von Dedekind herrührenden, für seine Theorie besonders wichtigen Satze:

Jedes Ideal $\mathfrak{a}$ ist der größte gemeinschaftliche Teiler zweier Hauptideale, und zwar kann jedes Ideal auf unendlich viele Arten so dargestellt werden.

Ist $\mathfrak{a}$ ein Hauptideal α, so sind diese Darstellungen $(\alpha\mu, \alpha\nu)$, wo $(\mu, \nu) \sim 1$. Ist aber $\mathfrak{a}$ kein Hauptideal, und α irgend ein durch $\mathfrak{a}$ teilbares Hauptideal, ferner $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ die Primteiler von α, so wird für jedes der unendlich vielen Hauptideale β, die wohl durch $\mathfrak{a}$, aber keines der Ideale $\mathfrak{a}\mathfrak{p}_1, \mathfrak{a}\mathfrak{p}_2, \ldots, \mathfrak{a}\mathfrak{p}_r$ teilbar sind, $(\alpha, \beta) \sim \mathfrak{a}$ sein*).

*) An die soeben auseinandergesetzte Theorie knüpft eine Reihe

Das Fundamentalsystem der wirklichen Größen eines Gattungsbereichs.

§ 14. Wenn der Gattungsbereich Γ aus $(\mathsf{A}, x_1, \ldots, x_m)$ durch Adjunktion einer Wurzel α der Gleichung

$$F_0 z^n + F_1 z^{n-1} + \cdots + F_n = 0$$

entsteht, ist α im allgemeinen keine ganze Größe, wohl aber $F_0\alpha$, da diese Größe der Gleichung

$$t^n + F_1 t^{n-1} + F_2 F_0 t^{n-2} + \cdots + F_n F_0^{n-1} = 0$$

genügt, die aus der vorigen entsteht, wenn man mit F_0^{n-1}

---

weiterer Problemstellungen an, die, wenn auch ohne weitere Ausführung, hier doch kurz erwähnt werden sollen.

Die im Texte benutzte Äquivalenz der idealen Größen ist im Sinne von Kap. I. § 5 als „absolute Äquivalenz" zu bezeichnen. Dem gegenüber bildet die Gesamtheit der Größen $\gamma\mathfrak{e}$, wo γ eine gegebene wirkliche ganze Größe des Gattungsbereichs, $\mathfrak{e}$ irgend eine ideale Einheit aus $[\mathfrak{G}]$ bezeichnet, d. h. die Gesamtheit der einer wirklichen ganzen Größe absolut äquivalenten Größen aus $[\mathfrak{G}]$ einen Äquivalenzbereich, der also (Kap. I. § 12) wieder eine relative Äquivalenz — nach Kroneckers Vorschlag eine Kummersche Äquivalenz — begründet. Diese relative Äquivalenz ergibt nun eine Klasseneinteilung der idealen Größen oder Ideale, die bisher nur für die Theorie der algebraischen Zahlen weiter ausgeführt wurde. In diesem einfachsten Falle ist die Anzahl der so entstehenden Klassen endlich; und das Problem der Bestimmung dieser Klassenzahl (siehe z. B. Dedekinds häufig citiertes Buch) das Fundamentalproblem der s. g. analytischen Zahlentheorie.

Eine weitere von Kronecker (Festschrift, § 22) angeregte Begriffsbildung, die aber bisher nicht weiter verfolgt wurde, bewegt sich gerade in entgegengesetzter Richtung, insofern sie auf einer Verschärfung des ursprünglichen Äquivalenzbegriffs beruht. Im Anschluß an § 7 dieses Kapitels können diese Untersuchungen dadurch charakterisiert werden, daß in den dort eingeführten Quotienten $\frac{\gamma_u}{\varepsilon_v}$ der Nenner ε_v nun eine eigentlich primitive Form sein soll. Als eigentlich primitive Form ist hier eine solche Form $\sum \varepsilon_r U_r$ zu verstehn, für welche die Koeffizienten ε_i, als Divisorensystem aufgefaßt, der im engeren Sinne genommenen Äquivalenz (Kap. VII. § 2)

$$(\varepsilon_1, \varepsilon_2, \ldots) \simeq 1$$

genügen.

multipliziert und $F_0 z = t$ setzt. Dabei ist unmittelbar zu sehn, daß mit α auch $F_0 \alpha$ eine algebraische Größe n^{ter} Ordnung ist.

Zur Definition des Gattungsbereichs Γ, sowie des in ihm enthaltenen Bereichs $[\Gamma]$ kann daher immer eine unmittelbar bekannte ganze Größe des Bereichs, γ, verwendet werden; und dies soll im folgenden durchweg geschehen.

Ist γ diese ganze Größe des Gattungsbereichs Γ, so wird jede Größe des Gattungsbereichs wieder in der Gestalt

$$\frac{G_0 + G_1 \gamma + \cdots + G_{n-1} \gamma^{n-1}}{H}$$

darstellbar sein, wo $G_0, G_1, \ldots, G_{n-1}$ und H (das $\neq 0$) Formen aus $[\mathsf{A}, x_1, \ldots, x_{m-1}]$ bedeuten. Ist $H = 1$, so ist jene Größe gewiß ganz; aber es muß durchaus nicht jede ganze Größe so darstellbar sein, daß $H = 1$ wird.

Es zeigt sich dies schon an dem einfachsten Beispiel jenes Gattungsbereichs, den man erhält, wenn man dem Bereiche (1) eine Wurzel der Gleichung $x^2 + 3 = 0$ adjungiert. Man sieht dann unmittelbar, daß die Größe

$$\frac{-1 + \sqrt{-3}}{2}$$

ganz ist, denn sie genügt der Gleichung $x^2 + x + 1 = 0$. Und es kann nicht

$$\frac{-1 + \sqrt{-3}}{2} = a + b\sqrt{-3}$$

sein, wo a und b gewöhnliche ganze Zahlen bedeuten. Hieraus würde nämlich

$$(2a + 1) + (2b - 1)\sqrt{-3} = 0,$$

also auch

$$2a + 1 = 0,\ 2b - 1 = 0$$

und im Gegensatz zur Annahme $a = -\frac{1}{2}$, $b = \frac{1}{2}$ folgen.

Um die allgemeine Gestalt der ganzen Größen in Γ festzustellen, sei μ eine beliebige solche ganze Größe; dann kann man jedenfalls

$$\mu = R_0 + R_1 \gamma + \cdots + R_{n-1} \gamma^{n-1}$$

schreiben, wenn man unter R Größen erster Ordnung aus Γ, d. h. Quotienten zweier Formen aus $[A, x_1, \ldots, x_m]$ versteht. Dasselbe findet aber in allen konjugierten Gattungsbereichen statt, und man hat daher zur Bestimmung der R das Gleichungssystem:

$$\mu_i = R_0 + R_1\gamma_i + \cdots + R_{n-1}\gamma_i^{n-1},$$
$$(i = 1, \ldots, n).$$

Bedenkt man, daß das Quadrat der aus den Koeffizienten der Unbekannten gebildeten Determinante bis auf das Vorzeichen geradezu die Discriminante der irreduzibeln Gleichung n^{ten} Grades für γ, also eine Form des Bereichs $[A, x_1, \ldots, x_m]$ ist, die wir mit D oder $D(\gamma)$ bezeichnen wollen (und auch kurz die Discriminante von γ nennen), so sieht man, daß

$$DR_i$$

ganz sein, also in dem Ausdruck $\frac{G_i}{H}$, wenn man den größten gemeinschaftlichen Teiler von G_i und H schon entfernt hat, H ein Teiler von D sein muß, oder endlich

$$R_i = \frac{G_i'}{D}$$

geschrieben werden kann.

Jede wirkliche ganze Größe des Gattungsbereichs Γ läßt sich mithin in der Gestalt

$$\mu = \frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D}$$

darstellen, wo D die Discriminante von γ, und daher D, sowie auch $G_0, \ldots, G_{n-1}$ Formen aus $[A, x_1, \ldots, x_m]$ sind.

Aus dieser Darstellung folgt aber eine Darstellung der ganzen Größen von Γ in Gestalt ganzer Formen, die von grundlegender Bedeutung ist.

Aus den Formensystemen $(G_0, G_1, \ldots, G_{n-1})$, die bei der Darstellung sämtlicher ganzen Größen zur Verwendung ge-

langen, läßt sich nämlich nach dem Satze*) in Kap. VII. § 5 eine endliche Anzahl von Formen

$$G_0^{(i)}, G_1^{(i)}, \ldots, G_{n-1}^{(i)}$$
$$(i = 1, \ldots, r)$$

so wählen, daß für jedes weitere System

$$G_0, G_1, \ldots, G_{n-1}$$

Relationen von der Gestalt

$$G_j = \sum_{i=1}^{r} H_i G_j^{(i)}$$

bestehn.

Sind also

$$\mu_i = \frac{G_0^{(i)} + G_1^{(i)}\gamma + \cdots + G_{n-1}^{(i)}\gamma^{n-1}}{D}$$
$$(i = 1, \ldots, r)$$

r bestimmte ganze Größen des Gattungsbereichs Γ, so läßt sich jede weitere wirkliche ganze Größe aus Γ in der Gestalt

$$\mu = \sum_{i=1}^{r} H_i \mu_i$$

schreiben, wo H_i Formen des Bereichs $[A, x_1, \ldots, x_m]$ sind. Daß auch jede solche Größe eine ganze Größe des Gattungsbereichs darstellt, ist evident.

Jedes solche System $\mu_1, \ldots, \mu_r$ soll als ein Fundamentalsystem der Gattung bezeichnet werden. Dabei kann dieses Fundamentalsystem insofern auf seine notwendigen Elemente beschränkt werden, daß, wenn z. B. für μ_r eine Relation

$$\mu_r = \sum_{i=1}^{r-1} H_i' \mu_i$$

---

*) Wenn man genau so wie in Kap. VII. § 6 die Formen $G_0^{(i)}, G_1^{(i)}, \ldots$ mit Hilfe der neuen Unbestimmten $u_0, u_1, \ldots$ in

$$G^{(i)} = G_0^{(i)} u_0 + G_1^{(i)} u_1 + \cdots$$

zusammenfaßt.

besteht, dieses Element einfach wegbleibt. Ob irgend ein μ in dieser Weise weggelassen werden kann, wird, wie man sieht, durch die Auflösung eines Systems linearer Gleichungen entschieden.

Eine andere, viel tiefer liegende Frage, die bisher in dieser Allgemeinheit nicht untersucht wurde, ist die nach der kleinsten Anzahl von Elementen, die in einem Fundamentalsysteme auftreten müssen.

Jedenfalls ist die Anzahl der Elemente des Fundamentalsystems $r \geqq n$, die Ordnung der Gattung.

Im entgegengesetzten Falle würde nämlich aus

$$\gamma^j = \sum_{i=1}^{r} H_{ij}\mu_i, \qquad (j = 0, \cdots, r)$$

eine Gleichung vom höchstens $n - 1^{\text{ten}}$ Grade mit nicht durchweg verschwindenden Koeffizienten für γ folgen, was unmöglich, da ja γ eine algebraische Größe n^{ter} Ordnung ist.

§ 15. Um ein Fundamentalsystem der in Bezug auf den orthoiden Bereich A relativ ganzen Größen eines aus $(\mathsf{A}, x_1, \ldots, x_m)$ entstammenden Gattungsbereichs aufzustellen, gehn wir wieder von der (durch die Definition des Gattungsbereichs selbst unmittelbar gegebenen) ganzen Größe γ des Gattungsbereichs aus. Die Discriminante von γ sei D; diese ist, wie wir wissen, eine Form aus $[\mathsf{A}, x_1, \ldots, x_m]$.

Jede (relativ) ganze Größe des Gattungsbereichs ist in der Gestalt

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D} \qquad (1)$$

darstellbar; wäre also $D \sim 1$, so ergäbe sich unmittelbar $1, \gamma, \ldots, \gamma^{n-1}$ als Fundamentalsystem. Wir haben daher nur den Fall näher zu untersuchen, wo D die Unbestimmten x wirklich enthält.

Dabei kommt es darauf an, die Formen G aus $[\mathsf{A}, x_1, \ldots, x_m]$ in allgemeinster Weise so zu bestimmen, daß jene Größe ganz werde. Dann müssen vor allem die Größen

$$\frac{G_0 + G_1\gamma_i + \cdots + G_{n-1}\gamma_i^{n-1}}{D}, \quad (i = 1, \ldots, n)$$

aus Γ_i, $(i = 1, \ldots, n)$ ganze Größen sein, und ebenso die elementaren symmetrischen Formen dieser Größen, die

$$\frac{S_1}{D}, \frac{S_2}{D^2}, \ldots, \frac{S_n}{D^n}$$

geschrieben werden können, wo S_j eine homogene Form j^{ter} Dimension von $G_0, G_1, \ldots, G_{n-1}$ mit Koeffizienten aus $[\mathsf{A}, x_1, \ldots, x_m]$ ist. Die statuierte Bedingung ist, wie man unmittelbar sieht, auch hinreichend; denn die als ganz zu erweisende Größe genügt dann in der Tat einer Gleichung von entsprechender Gestalt.

Unser Problem läßt sich also dahin fassen, daß in den homogenen Formen j^{ter} Dimension S_j $(j = 1, \ldots, n)$ die „unbekannten" Formen G so zu bestimmen sind, daß S_j durch D^j teilbar sei; die Teilbarkeit ist auf den Bereich $[\mathsf{A}, x_1, \ldots, x_m]$ zu beziehen.

Eine lineare Transformation der Unbestimmten x, deren Determinante gleich Eins, und deren Koeffizienten rationale und ganze Zahlen sind, und die — wie man unmittelbar sieht — an der Problemstellung nichts ändert, wird D in eine reguläre Form der x überführen, deren Dimension r sei. Dabei ist $r \neq 0$, da der Fall $D \sim 1$ als schon erledigt betrachtet werden kann.

Nach dieser linearen Transformation kann man

$$G_i = DQ_i + G_i'$$
$$G_i' = \sum_{h=0}^{r-1} G_{ih} x_m^h$$

schreiben, wo die G_{ih} nur mehr Formen aus $[\mathsf{A}, x_1, \ldots, x_{m-1}]$ (für $m = 1$ Größen aus A) sind. Die Formen $G_0, \ldots, G_{n-1}$ ergeben dann und nur dann ganze Größen in (1), wenn dies

für $G_0', \ldots, G_{n-1}'$ der Fall ist. In der letzten Fassung des Problems kann man also geradezu die unbekannten Formen als Formen $r - 1^{\text{ten}}$ Grades in x_m voraussetzen; und die Tatsache der Teilbarkeit durch D^j wird sich demnach durch ein System diophantischer Gleichungen in $[\mathsf{A}, x_1, \ldots, x_{m-1}]$ ausdrücken, deren Grad jedoch bis zum n^{ten} ansteigt. Als „Unbekannte" treten in diesen Gleichungen die Formen G_{ih} und nur diese auf; nicht aber vielleicht auch die unbekannten Koeffizienten der Quotienten, deren Existenz vorausgesetzt wird. Man erkennt dies unmittelbar, wenn man die fraglichen Teilbarkeitsbedingungen im Sinne des Kap. III. § 1 u. 2 durch das gewöhnliche Divisionsverfahren herstellt.

Dieselben Teilbarkeitsbedingungen können aber noch ganz anders interpretiert werden. Wenn man statt A das Reich der aus $(\mathsf{A}, x_1, \ldots, x_{m-1})$ entstammenden algebraischen Größen, mit einer schon gebrauchten Bezeichnung $\{\mathsf{A}, x_1, \ldots, x_{m-1}\}$, zu Grunde legt, so werden die Bedingungen dafür, daß die Größen

$$\frac{G_0' + G_1'\gamma_i + \cdots + G_{n-1}'\gamma_i^{n-1}}{D}, \quad (i = 1, \ldots, n)$$

in Bezug auf $\{\mathsf{A}, x_1, \ldots, x_{m-1}\}$ relativ ganz seien, wenn man jetzt unter G_{ih} beliebige Größen dieses Bereichs versteht, genau durch dieselben Gleichungen ausgedrückt wie früher.

Dieses Gleichungssystem hat aber die evidente Eigenschaft, daß mit den Systemen $G_{ih}^{(1)}$ und $G_{ih}^{(2)}$ auch das System $uG_{ih}^{(1)} + vG_{ih}^{(2)}$ eine Lösung davon ist, wie immer auch u und v aus $\{\mathsf{A}, x_1, \ldots, x_{m-1}\}$ gewählt werden mögen. Man kann also darauf die in Kap. V. § 12 und 13 erhaltenen Resultate anwenden und damit festsetzen, daß die Minimalresolvente in Bezug auf die Unbekannten G_{ih} linear sein muß. Diese wird aber durch rationale Operationen aus den vorgelegten Gleichungen erhalten, und es wird demnach der Inhalt des untersuchten Gleichungssystems mit dem Inhalt eines Gleichungssystems vollständig übereinstimmen, das in Bezug auf die G_{ih}' linear ist und dessen Koeffizienten Formen aus $[\mathsf{A}, x_1, \ldots, x_{m-1}]$ sind. Sollen nun Formen aus $[\mathsf{A}, x_1, \ldots, x_{m-1}]$

jenen Gleichungen genügen, so müssen sie auch dieser linearen Gleichung genügen, und umgekehrt.

Die Bestimmung der G_{ih} wird daher einfach durch ein System linearer diophantischer Gleichungen in $[\mathsf{A}, x_1, \ldots, x_{m-1}]$ gegeben; und die Gesamtheit der in Bezug auf A relativ ganzen Größen des Gattungsbereichs Γ durch die lineare Form

$$H_1\mu_1 + H_2\mu_2 + \cdots$$

dargestellt, wenn $H_1, H_2, \ldots$ beliebige Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ sind.

Man erhält das Fundamentalsystem, wenn man in

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D}$$

die allgemeine Lösung für $G_0, G_1, \ldots$ einsetzt und nach den in diesen auftretenden unbestimmten Formen ordnet, als das System der Koeffizienten dieser Formen. Diese sind ganze Größen, denn sie entsprechen der Wahl $H_i = 1$, wenn alle übrigen H gleich Null gesetzt werden.

Die soeben auseinandergesetzte Methode ist in Kroneckers Festschrift (§ 6) kurz angedeutet. Nach einer dort hinzugefügten Bemerkung ist die Methode „auch anzuwenden", wenn es sich um das Fundamentalsystem absolut ganzer Größen handelt. Für eine solche Anwendung der Methode würde es aber neuer theoretischer Hilfsmittel, insbesondere einer (sehr komplizierten) Darstellung der allgemeinen Eliminationstheorie für Kongruenzensysteme bedürfen. Auf diese Entwicklungen gehe ich nicht ein, weil mit den Eliminationsmethoden ein fremdes und jedenfalls überflüssiges Element in die Behandlung des Problems eingeführt wird, und zwar nicht nur in die Theorie, sondern auch in die Praxis der Herstellung des Fundamentalsystems. Statt dessen werden wir eine andere, wesentlich einfachere Methode für die Lösung des vorgelegten Problems geben, die außerdem für relativ und absolut ganze Größen völlig identisch ist. Nur der einfachste

Grenzfall, wenn der Gattungsbereich aus algebraischen Zahlen besteht, entzieht sich ihr und soll deshalb zuerst für sich abgehandelt werden.

§ 16. Für den durch die ganze algebraische Zahl γ definierten Gattungsbereich (γ) ist jede Größe dieses Bereichs in Bezug auf (1) relativ ganz, und wenn γ eine algebraische Zahl n^{ter} Ordnung ist, jede Größe des Bereichs gewiß in der Gestalt

$$r_0 + r_1\gamma + \cdots + r_{n-1}\gamma^{n-1}$$

darstellbar, wenn die r entsprechend gewählte rationale Zahlen sind.

Für die Herstellung eines Fundamentalsystems der absolut*) ganzen algebraischen Zahlen des Bereichs (γ) besteht nun ein sehr einfaches Verfahren, das wohl in allen die Theorie der algebraischen Zahlen behandelnden Werken zu finden ist, hier aber doch reproduziert werden muß, weil die nachher zu gebende allgemeine Methode gerade für diesen einfachsten Fall versagen kann.

Ist die Discriminante von γ gleich d, so ist jede ganze Zahl des Bereichs gewiß in der Gestalt

$$\frac{g_0 + g_1\gamma + \cdots + g_{n-1}\gamma^{n-1}}{d}$$

darstellbar: man hat also wie früher aus Zahlen dieser Form die ganzen Zahlen auszuwählen. Die g und d sind rationale und ganze Zahlen. Nennt man k_i den kleinsten, nicht negativen Rest von $g_i \pmod{d}$, so ist die allgemeinste Gestalt jener Zahlen

$$a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1} + \frac{k_0 + k_1\gamma + \cdots + k_{n-1}\gamma^{n-1}}{d},$$

wo die a beliebige rationale und ganze Zahlen bedeuten, während $k_0, k_1, \ldots, k_{n-1}$ nur die Werte $0, 1, \ldots, d-1$ annehmen können.

*) Der Zusatz „absolut" wird in diesem Falle als selbstverständlich wegzulassen sein, da eben jede algebraische Zahl „relativ" ganz ist.

Die Zahlen $1, \gamma, \ldots, \gamma^{n-1}$ mit den in endlicher Anzahl vorhandenen ganzen Zahlen der Gestalt

$$\frac{k_0 + k_1\gamma + \cdots + k_{n-1}\gamma^{n-1}}{d}$$

bilden augenscheinlich ein Fundamentalsystem.

Daß man aus diesem auch immer in einfachster Weise ein genau n Elemente enthaltendes Fundamentalsystem erhalten kann, ist schon ein der speziellen Theorie der algebraischen Zahlen angehöriger Satz, der eben deshalb hier nicht weiter ausgeführt wird*).

Teilbarkeit der Formen nach einem Äquivalenzmodul.

§ 17. Um die definitive Lösung der ferner zu erledigenden allgemeinen Grundprobleme in der arithmetischen Theorie der algebraischen Größen möglichst einfach zu formulieren, ist endlich noch eine — die letzte — neue Begriffsbestimmung einzuführen, die jetzt besprochen werden soll. In irgend einem vollständigen holoiden Bereiche definiert die Gesamtheit jener Größen $\mathfrak{r}$, deren größter gemeinschaftlicher Teiler mit einer gegebenen Größe $\mathfrak{m}$ die Eins ist, im Sinne von Kap. I. § 12 einen Äquivalenzbereich, der als der Größe $\mathfrak{m}$ zugeordnet bezeichnet werden kann. Diese Größe $\mathfrak{m}$, die jetzt zu gleicher Zeit einen Kongruenzbereich und einen Äquivalenzbereich bestimmen wird, soll von nun ab Äquivalenzmodul genannt werden. Zwei jenem vollständigen holoiden Bereiche entstammende Formen $\mathfrak{A}_1$ und $\mathfrak{A}_2$ sollen nach dem Äquivalenzmodul $\mathfrak{m}$ — (aequ. mod. $\mathfrak{m}$) — äquivalent genannt werden, wenn es zwei Größen jenes Äquivalenzbereichs $\mathfrak{r}_1$ und $\mathfrak{r}_2$ gibt, so daß

*) Ein dieser Schlußreihe genau analoges Verfahren ist auch dann noch anwendbar, wenn wir es mit dem Bereiche (A, x) entstammenden Gattungsbereichen zu tun haben, wo A ein orthoider Bereich ist, insbesondere also in der Theorie der algebraischen Funktionen einer Veränderlichen, wenn von den Zahlenkoeffizienten abgesehn wird (siehe Kronecker, Festschrift, § 7).

$$\mathfrak{r}_1 \mathfrak{A}_1 \equiv \mathfrak{r}_2 \mathfrak{A}_2 \pmod{\mathfrak{m}}$$

wird; eine Beziehung, die, wenn es auf die Größen $\mathfrak{r}_1$ und $\mathfrak{r}_2$ nicht ankommt, durch

$$\mathfrak{A}_1 \sim \mathfrak{A}_2 \text{ (aequ. mod. } \mathfrak{m})$$

angedeutet werde.

Ferner soll $\mathfrak{A}_1$ aequ. mod. $\mathfrak{m}$ durch $\mathfrak{A}_2$ teilbar heißen, wenn es zwei Größen jenes Äquivalenzbereichs $\mathfrak{r}_1$ und $\mathfrak{r}_2$ gibt, so daß

$$\mathfrak{r}_1 \mathfrak{A}_1 \equiv \mathfrak{r}_2 \mathfrak{A}_2 \mathfrak{A}_3 \pmod{\mathfrak{m}}$$

wird, wo auch $\mathfrak{A}_3$ eine jenem vollständigen holoiden Bereiche entstammende Form ist.

Die Teilbarkeit nach dem Äquivalenzmodul $\mathfrak{m}$ ist von der Teilbarkeit nach dem Modul (Kongruenzmodul) $\mathfrak{m}$ wohl zu unterscheiden. Es ist, wie schon früher, $\mathfrak{A}_1$ durch $\mathfrak{A}_2$ (mod. $\mathfrak{m}$) teilbar, wenn es eine dritte Form $\mathfrak{A}_3$ gibt, so daß

$$\mathfrak{A}_1 \equiv \mathfrak{A}_2 \mathfrak{A}_3 \pmod{\mathfrak{m}};$$

während die Teilbarkeit aequ. mod. $\mathfrak{m}$ nach der neu eingeführten Bezeichnung durch

$$\mathfrak{A}_1 \sim \mathfrak{A}_2 \mathfrak{A}_3 \text{ (aequ. mod. } \mathfrak{m})$$

ausgedrückt wird.

Die in Kap. I. § 5 angeführten drei Grundgesetze der Rechnung mit Äquivalenzen behalten, wie man sehr leicht sieht, auch jetzt ihre Geltung, mit der einzigen Modifikation, daß in III nicht bloß die Null, sondern jede Größe $\mathfrak{B}$ auszuschließen ist, für die $(\mathfrak{B}, \mathfrak{m})$ nicht ~ 1; für irreduzible $\mathfrak{m}$ insbesondere also jede Größe $\mathfrak{B}$, die $\equiv 0 \pmod{\mathfrak{m}}$.

Diese Begriffsbestimmungen sollen auf den Fall angewendet werden, wo der vorgelegte vollständige holoide Bereich $[\mathsf{A}, x_1, \ldots, x_m]$ ist und A, wie immer, entweder einen orthoiden Bereich oder [1] bedeutet; wir werden es demnach mit diesem Bereiche entstammenden Formen der neuen Unbestimmten $z_1, z_2, \ldots$ zu tun haben. Der Modul P soll aber jetzt eine echte irreduzible Größe des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ sein.

Eine dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form G der neuen Unbestimmten $z_1, z_2, \ldots$ soll wieder aequ. mod. P ein echter Teiler von F sein, wenn F durch G teilbar aequ. mod. P, aber G weder der Einheit, noch der Form F selbst nach dem Äquivalenzmodul P äquivalent ist.

Eine Form G, die ~ 1 (aequ. mod. P) ist, für die also

$$e_1 G \equiv e_2 \text{ (mod. } P)$$

wird, wo e_1 und e_2 zu P teilerfremde Größen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ sind, muß offenbar selbst auch einer zu P teilerfremden Größe dieses Bereichs mod. P kongruent sein. Ist also

$$G \sim G_1 G_2 \text{ und } G_1 \sim 1 \text{ (aequ. mod. } P),$$

so muß auch

$$G_2 \sim G \text{ (aequ. mod. } P)$$

sein, was übrigens auch aus dem dritten Grundgesetze für Äquivalenzen unmittelbar folgt.

Eine Form G, die nach dem Äquivalenzmodul P keinen echten Teiler besitzt, soll wieder als aequ. mod. P irreduzible Form bezeichnet werden. Man hat dann den Satz: Eine Form G ist nach dem Äquivalenzmodul P gewiß nicht irreduzibel, wenn sie mod. P als Produkt zweier die Unbestimmten z wirklich*) enthaltenden Formen dargestellt werden kann.

Aus der Kongruenz

$$G \equiv G_1 G_2 \text{ (mod. } P),$$

wo G_1, G_2 die Unbestimmten z enthaltende Formen sind, folgt sofort

$$G \sim G_1 G_2 \text{ (aequ. mod. } P),$$

und es ist nach der für G_1 und G_2 geltenden Annahme weder G_1 noch $G_2 \sim 1$.

*) Dieser kurze Ausdruck bedeutet eine solche Form, in der irgend ein Potenzprodukt der z, das nicht Eins, einen mod. P von Null verschiedenen Koeffizienten besitzt.

§ 18. In der auf den Äquivalenzmodul P bezogenen Teilbarkeitstheorie der Formen, wo P eine echte irreduzible Größe des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ bedeutet, haben wir den fundamentalen Satz nachzuweisen, daß jede aequ. mod. P echte irreduzible Form auch eine Primform ist, d. h. daß für eine solche Form G jedes Produkt $F_1 F_2$ nur dann aequ. mod. P durch G teilbar sein kann, wenn dies schon für einen der Faktoren F_1 oder F_2 stattfindet.

Dabei wird der Fall, wo P eine gewöhnliche Primzahl p ist, gesondert zu betrachten sein. Dann ist $\mathsf{A} = [1]$, da für einen orthoiden Bereich A jede rationale Zahl, also auch $p \sim 1$ wäre.

In diesem (ersten) Falle folgt aus der Äquivalenz

$$F_1 F_2 \sim GH \text{ (aequ. mod. } p)$$

die Kongruenz

$$e_1 F_1 F_2 \equiv e_2 GH \text{ (mod. } p).$$

Nun ist G, das die Unbestimmten z wirklich enthält, jedenfalls mod. p in der Gestalt $e_3 G_1$ darstellbar, wo G_1 eine mod. p primitive Form der z ist und die Unbestimmten z wieder wirklich enthält. Dann muß weiter G_1 auch mod. p irreduzibel, also auch mod. p eine Primform sein*), und e_1, das die z nicht enthält, ist gewiß nicht durch G_1 teilbar. Dies muß demnach für $F_1 F_2$, also endlich auch für F_1 oder F_2 der Fall sein. Es ist also z. B.

$$F_1 \equiv G_1 H_1, \; e_3 F_1 \equiv GH \text{ (mod. } p),$$

mithin auch

$$F_1 \sim GH_1 \text{ (aequ. mod. } p).$$

Aus den soeben gegebenen Entwicklungen folgt noch unmittelbar der Satz:

Ist der Äquivalenzmodul eine gewöhnliche Primzahl p, so ist eine Form G dann und nur dann aequ. mod. p irreduzibel, wenn sie mod. p irreduzibel ist.

---

*) Die Theorie der Teilbarkeit der Formen nach einem Primzahlmodul p ist ganz elementarer Natur und unter der im vorhergehenden Kapitel behandelten Theorie der P-Systeme enthalten.

Daß die Irreduzibilität mod. p eine Folge der entsprechenden Eigenschaft aequ. mod. p ist, haben wir schon früher (§ 17) erschlossen; ist umgekehrt G irreduzibel mod. p, so folgt die Unmöglichkeit einer Darstellung als Produkt aequ. mod. p, dessen Faktoren die z wirklich enthaltenden Formen sind, d. h. die Unmöglichkeit der Äquivalenz

$$G \sim G_1 G_2 \text{ (aequ. mod. } p)$$

leicht, wenn man G, G_1, G_2 als Produkt einer zu p teilerfremden Größe des Bereichs $[A, x_1, \ldots, x_m]$ und einer mod. p primitiven Form der z schreibt. Seien die letzteren Formen G', G_1', G_2', die aequ. mod. p mit G, resp. G_1 und G_2 aequivalent sind. Dann hat man

$$e_1 G' \equiv e_2 G_1' G_2' \text{ (mod. } p),$$

und es muß nun, weil G' und $G_1' G_2'$ primitiv sind, endlich

$$G' \equiv \pm G_1' G_2' \text{ (mod. } p)$$

sein, es wäre also auch G' und damit auch G nicht irreduzibel mod. p.

Jede Form, die nicht ~ 0 oder 1 (aequ. mod. p), ist also aequ. mod. p als Produkt von nach dem Äquivalenzmodul p irreduzibeln Formen darstellbar, und diese Darstellung ist im Sinne der Äquivalenzbestimmung eindeutig bestimmt.

Das letztere ergibt sich aus dem Umstande, daß aequ. mod. p echte irreduzible Formen auch Primformen sind. Die Darstellung selbst folgt unmittelbar aus der Zerlegung mod. p, wo nur die z nicht enthaltenden Teiler, die jetzt ~ 1 sind, weggelassen werden können, also jeder wirkliche Teiler jetzt aequ. mod. p in der kanonischen Gestalt einer mod. p primitiven Form geschrieben werden kann.

§ 19. Ganz anders ist vorzugehn, wenn die irreduzible Form P wenigstens eine der Unbestimmten x, z. B. x_1 wirklich enthält. Wir fassen dann in der gleichfalls irreduzibeln Gleichung:

$$P(x_1, \ldots, x_m) = 0$$

x_1 als Unbekannte, die übrigen x als Unbestimmte. Diese Gleichung definiert einen aus $(\mathsf{A}, x_1, \ldots, x_m)$ entstammenden Gattungsbereich (ξ), wo wir unter ξ eine solche Größe des Gattungsbereichs verstehn, für die $P(\xi, \ldots) = 0$ wird.

Jede Kongruenz $A \equiv B \pmod{P}$ ergibt dann eine Identität $[A]_\xi = [B]_\xi$, wo das Zeichen $[\cdots]_\xi$ die Ersetzung von x_1 durch ξ andeutet.

Jede Größe des Gattungsbereichs (ξ) kann in der Gestalt $\frac{[A]_\xi}{E}$ geschrieben werden, wo A und E Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ sind, von denen die erste in x_1 den $n - 1^{\text{ten}}$ Grad nicht übersteigt, die zweite x_1 überhaupt nicht enthält. Ist demnach F irgend eine dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form der z, so erhält man für F eine Beziehung

$$E[F]_\xi - [\Psi]_\xi = 0,$$

wo E eine Form aus $[\mathsf{A}, x_2, \ldots, x_m]$ und Ψ eine Form der x und z, die in x_1 den Grad $n - 1$ nicht übersteigt. Es ist also $EF - \Psi$ jedenfalls in dem Sinne durch P teilbar, daß dabei noch die Unbestimmten $x_2, \ldots$ enthaltende Nenner auftreten könnten. Da aber nicht nur die Gleichung $P = 0$, sondern auch schon die Form P irreduzibel ist, d. h. auch keinen von x_1 unabhängigen Teiler besitzt, hat man schließlich

$$EF - \Psi \equiv 0 \pmod{P}.$$

Ist endlich Ψ als Form der z nicht primitiv, also $\Psi = E_1 \Phi$, so hat man schließlich

$$F \sim \Phi \text{ (aequ. mod. } P).$$

Man hat damit für F eine ihr (aequ. mod. P) äquivalente Form von kanonischer Gestalt, Φ, gefunden, die eine in x_1 den $n - 1^{\text{ten}}$ Grad nicht übersteigende primitive Form der z ist. Es sind nun zwei Formen F_1 und F_2 dann und nur dann aequ. mod. P äquivalent, wenn $[\Phi_1]_\xi$ und $[\Phi_2]_\xi$ im Gattungsbereiche (ξ) äquivalent sind.

Aus $F_1 \sim F_2$ (aequ. mod. P) folgt $\Phi_1 \sim \Phi_2$ (aequ. mod. P) oder

$$A_1 \Phi_1 \equiv A_2 \Phi_2 \text{ (mod. } P);$$

also

$$[A_1]_\xi [\Phi_1]_\xi = [A_2]_\xi [\Phi_2]_\xi,$$

d. h. $[\Phi_1]_\xi$ und $[\Phi_2]_\xi$ unterscheiden sich nur durch Multiplikation mit von 0 verschiedenen Größen aus (ξ) und sind demnach äquivalent. Da die angeführten Schlüsse sich augenscheinlich auch in der umgekehrten Reihenfolge ausführen lassen, ist der angeführte Satz bewiesen.

Eine von 0 verschiedene Form Φ, die kein z enthält, ist ~ 1 (aequ. mod. P), da Φ vom höchstens $n - 1^{\text{ten}}$ Grade, also relativ prim zu P ist.

Wenn wir zum Beweise des am Anfang von § 18 ausgesprochenen Satzes zurückkehren, und der Annahme nach

$$F_1 F_2 \sim G H \text{ (aequ. mod. } P)$$

ist, kann man die sämtlichen Formen in der ihnen äquivalenten oben charakterisierten Gestalt geschrieben denken und hat dann die Identität:

$$[e_1 F_1 F_2]_\xi = [e_2 G H]_\xi.$$

Ist aber G irreduzibel aequ. mod. P, so ist gewiß auch $[G]_\xi$ im Gattungsbereiche (ξ) irreduzibel. Eine echte Zerlegung ergäbe ja unmittelbar eine Darstellung aequ. mod. P von G als Produkt zweier die z wirklich enthaltenden Formen. Es muß also $[F_1]_\xi$ oder $[F_2]_\xi$ durch $[G]_\xi$ teilbar sein. Hat man z. B. $[F_1]_\xi = [G]_\xi \overline{H}$, so kann man die Form $\overline{H}$ der z wieder so schreiben, daß die Nenner nur mehr $x_2, \ldots, x_m$ enthalten, und es wird dann endlich, wenn der Zähler $[H]_\xi$ geschrieben wird,

$$F_1 \sim G H \text{ (aequ. mod. } P),$$

w. z. b. w.

Aus diesen Entwicklungen folgt weiter der Satz:

Ist der Äquivalenzmodul P eine Form der Unbestimmten, die z. B. x_1 wirklich enthält, so ist eine Form G dann und nur dann aequ. mod. P irreduzibel,

wenn $[G]_\xi$ in dem durch eine Wurzel der Gleichung $P = 0$ (mit der Unbekannten x_1) definierten Gattungsbereiche (ξ) irreduzibel ist*).

---

*) Also durchaus nicht, wenn G mod. P irreduzibel ist. Dieser wichtige Unterschied zwischen den beiden für den Äquivalenzmodul unterschiedenen Fällen, auf den wir noch zurückkommen, soll hier besonders betont sein. Im allgemeinen sind bei der Zerlegung mod. P irreduzible Formen durchaus nicht immer Primformen. Das ist nur in den der Theorie der algebraischen Zahlen und der algebraischen Funktionen einer Unbestimmten, wenn von den Zahlenkoeffizienten abgesehn wird, der Fall. Hier stimmt auch die Irreduzibilität mod. P und aequ. mod. P überein.

So ist z. B.

$$F = z_1^2 - 2 z_1 z_2 + z_2^2 - x z_1 z_3 + x z_2 z_3 + t z_3^2$$

nach dem Äquivalenzmodul $x^2 - 4t$, wo x und t Unbestimmte bedeuten, reduzibel; denn es ist

$$F \sim (2 z_1 - 2 z_2 - z_3 x)^2 \text{ (aequ. mod. } x^2 - 4 t),$$

weil

$$4 F \equiv (2 z_1 - 2 z_2 - z_3 x)^2 \text{ (mod. } x^2 - 4 t).$$

Dagegen ist F irreduzibel mod. $x^2 - 4t$ in dem Sinne, daß es nicht als Produkt zweier rationalen und ganzen Formen mod. $x^2 - 4t$ darstellbar ist. Denn es müßten dann rationale und ganze Formen X von x und t existieren, für welche

$$4 (X_1 z_1 + X_2 z_2 + X_3 z_3)(X_1' z_1 + X_2' z_2 + X_3' z_3') \equiv (2 z_1 - 2 z_2 - z_3 x)^2 \text{ (mod. } x^2 - 4 t)$$

wäre. Setzt man in der dieser Kongruenz entsprechenden Identität

$$t = u^2, \quad x = 2 u,$$

so erhält man die weitere Identität

$$(\overline{X}_1 z_1 + \overline{X}_2 z_2 + \overline{X}_3 z_3)(\overline{X}_1' z_1 + \overline{X}_2' z_2 + \overline{X}_3' z_3) = (z_1 - z_2 - u z_3)^2,$$

wo $\overline{X}$ eine rationale und ganze Form von u bedeutet, die aus X durch die angegebene Substitution entsteht. Da aber auch X rationale und ganze Koeffizienten besaß, sieht man unmittelbar, daß in jedem $\overline{X}$ der Koeffizient der ersten Potenz von u eine gerade Zahl sein muß.

Andrerseits müßte, wegen der eindeutigen Zerlegung von $(z_1 - z_2 - u z_3)^2$ in rationale und ganze Primformen, im Gegensatze mit der für $\overline{X}_3$ eben statuierten Eigenschaft,

$$\overline{X}_3' = \pm u$$

sein. Die vorausgesetzte Zerlegung ist also in der Tat unmöglich.

Daß aus der Irreduzibilität von G nach dem Äquivalenzmodul P immer auch die Irreduzibilität von $[G]_\xi$ im Gattungsbereiche (ξ) folgt, wurde schon früher erwähnt. Ist umgekehrt $[G]$ irreduzibel in (ξ), so führt die Annahme

$$G \sim G_1 G_2 \text{ (aequ. mod. } P),$$

wo G_1 und G_2 die z wirklich enthaltende Formen sein sollen, zu einem Widerspruche. Es wäre dann auch

$$EG \equiv E_1 G_1 G_2 \text{ (mod. } P),$$

wo E, E_1 durch P nicht teilbare Formen aus $[\mathsf{A}, x_1, \ldots, x_m]$ sind; und weiter

$$[G]_\xi = \eta [G_1]_\xi [G_2]_\xi,$$

wo η eine von 0 verschiedene Größe des Gattungsbereichs (ξ) ist, also müßte eine wirkliche Zerlegung von $[G]_\xi$ vorhanden sein.

Jede Form, die nicht ~ 0 oder 1 (aequ. mod. P), ist also — gerade so wie früher für den Fall einer gewöhnlichen Primzahl — aequ. mod. P als Produkt von nach dem Äquivalenzmodul P irreduzibeln Formen darstellbar, und diese Darstellung ist im Sinne der Äquivalenzbestimmung eindeutig bestimmt.

Das letztere ist eine Folgerung aus der Tatsache, daß aequ. mod. P echte irreduzible Formen auch immer Primformen sind. Die Darstellung selbst ergibt sich unmittelbar aus der Zerlegung von $[G]_\xi$ im Gattungsbereiche (ξ), in welcher nur die Nenner, von x_1 unabhängige Formen, durch Multiplikation zu entfernen sind, also die Faktoren in der früher erörterten kanonischen Gestalt geschrieben werden können.

§ 20. Wie die nun abgeschlossene Theorie der Zerlegung einer Form zeigt, ist die Einführung des „Äquivalenzmoduls" prinzipiell nicht unbedingt notwendig, da die betreffenden Begriffsbestimmungen schließlich auch ohne diese neue Ausdrucksweise formuliert werden könnten. Dasselbe findet aber bei jeder Erweiterung der mathematischen Symbolik statt, und es wird immer zu erwägen sein, wie weit die Einführung des

neuen Symbols zweckmäßig ist. In Bezug auf den Äquivalenzmodul ist dies in hohem Maße der Fall. Ohne ein Eingehn in die hier in Frage kommenden Eigenschaften der Formen ist eine Lösung der Fundamentalprobleme der arithmetischen Theorie der algebraischen Größen überhaupt nicht möglich; wollte man trotzdem die der neuen Äquivalenzbestimmung entsprechenden Bezeichnungen vermeiden, so würde die ganze Darstellung nicht nur äußerst schwerfällig und undurchsichtig werden, sondern es müßten auch immer die beiden bisher unterschiedenen Fälle gesondert behandelt werden. Eine einheitliche Theorie kann also die neue Ausdrucksweise nicht vermeiden. In dieser erhalten wir noch außer dem soeben gegebenen grundlegenden Theoreme die folgenden für die Anwendungen wichtigen Sätze.

Es sei G eine dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form von $z, z_1, z_2, \ldots$, die mod. P regulär in Bezug auf z ist. Es sei ferner die Zerlegung von G nach dem Äquivalenzmodul P:

$$G \sim G_1^{a_1} G_2^{a_2} \ldots G_r^{a_r} \text{ (aequ. mod. } P),$$

wo bei der jetzt gebrauchten Schreibweise $G_1, G_2, \ldots$ schon aequ. mod. P nicht äquivalente Formen bedeuten. Die Zerlegung von G enthält bei dieser Annahme dann und nur dann eine Primform mehrfach, wenn die Discriminante von G (nach z) mod. P verschwindet. Es sind dann ferner die Discriminanten der Primformen $G_1, G_2, \ldots$ (nach z), sowie die Resultanten irgend zweier verschiedener Primformen (nach z) durchweg mod. P von 0 verschieden.

Die angeführten Tatsachen sind evident, wenn der Äquivalenzmodul eine natürliche Primzahl ist, da wir es dann eben nur mit der Zerlegung der Form G (mod. p) zu tun haben.

Für den Fall eines Unbestimmte enthaltenden Äquivalenzmoduls sind die folgenden einfachen Betrachtungen anzustellen. Mehrfache Primfaktoren sind in G vorhanden, wenn solche bei der Zerlegung von $[G]_\xi$ im Gattungsbereiche (ξ) auftreten.

Auch $[G]_\xi$ ist regulär in Bezug auf z und besitzt also nur wieder in Bezug auf z reguläre Teiler. Mehrfache solche Teiler treten dann und nur dann auf, wenn die Discriminante von $[G]_\xi$ nach z verschwindet. Diese ist aber $[\text{Dscr. } G]_\xi$ und also dann und nur dann Null, wenn $\text{Dscr. } G \equiv 0 \pmod{P}$.

Wäre weiter $\text{Dscr. } G_1 \equiv 0 \pmod{P}$, so hätte man auch $\text{Dscr. } [G_1]_\xi = 0$; d. h. es wäre $[G_1]_\xi$ und auch G_1 keine Primform. Ebenso würde aus $\text{Res. } (G_1, G_2) \equiv 0 \pmod{P}$ auch $\text{Res. } ([G_1]_\xi, [G_2]_\xi) = 0$ folgen; da aber $[G_1]_\xi$ und $[G_2]_\xi$ irreduzible Formen sind, müßten $[G_1]_\xi$ und $[G_2]_\xi$ äquivalent sein, und es wäre im Gegensatze zur Annahme auch

$$G_1 \sim G_2 \text{ (aequ. mod. } P).$$

Allgemeine Methode zur Aufstellung der Fundamentalsysteme.

§ 21. Das nun zu lösende Problem kann folgendermaßen gefaßt werden:

Es sei wieder A ein orthoider Bereich oder aber der Bereich [1], P irgend eine irreduzible Größe des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ und wieder γ eine diesem Bereiche entstammende ganze algebraische Größe n^{ter} Ordnung. Es seien ferner $\varphi_1, \varphi_2, \ldots, \varphi_k$ wirkliche ganze Größen des durch γ definierten Gattungsbereichs (Γ). Dann sollen dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehörige Formen $X_1, \ldots, X_k$ so bestimmt werden, daß

$$\frac{X_1\varphi_1 + X_2\varphi_2 + \cdots + X_k\varphi_k}{P}$$

eine ganze Größe sei, und es ist noch insbesondere nachzuweisen, daß dies dann und nur dann der Fall ist, wenn

$$X_i = H_{i1}\,Y_1 + \cdots + H_{is}\,Y_s$$

ist, wo die H bestimmte, die Y beliebige Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ bedeuten.

Daß nach Lösung dieses Problems das Fundamentalsystem der wirklichen ganzen Größen aus (Γ) in einer endlichen Anzahl von Schritten aufgestellt werden kann, ist sehr leicht einzusehn.

Ist die Discriminante von γ in $[A, x_1, \ldots, x_m]$ in irreduzible Faktoren zerlegt

$$D = P_1 P_2 P_3 \ldots,$$

so muß, wenn in der Bezeichnung des § 14:

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D}$$

ganz sein soll, dies jedenfalls auch für

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{P_1}$$

der Fall sein. Der Annahme nach geschieht dies bei einer gewissen oben angegebenen Gestalt der G, also wenn

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{P_1} = \sum_{j=1}^{s} Y_j \frac{H_{0j} + H_{1j}\gamma + \cdots + H_{n-1,j}\gamma^{n-1}}{P_1}$$

wird, wie immer auch die Formen Y_j gewählt sind. Die Koeffizienten der Y_j in der eben hingeschriebenen Summe sind also ganze Größen, und es wird, wenn man sie kurz mit φ_j bezeichnet:

$$\frac{G_0 + G_1\gamma + \cdots + G_{n-1}\gamma^{n-1}}{D} = \frac{\sum_{j=1}^{s} \varphi_j Y_j}{P_2 P_3 \ldots}.$$

Es muß dann wieder

$$\frac{\sum_{j=1}^{s} \varphi_j Y_j}{P_2}$$

ganz sein. Dies ergibt nach dem als richtig angenommenen Satze nun eine ähnliche Bestimmung der Y, wie früher der G. Fährt man so fort, bis alle irreduziblen Faktoren von D entfernt sind (unter denen auch gleiche vorkommen können), so erhält man schließlich alle wirklichen ganzen Größen des Gattungsbereichs in der Gestalt

$$\Sigma \Psi_j Y_j^{(r)},$$

wo die Ψ bestimmte ganze Größen, die $Y_j^{(r)}$ beliebige Formen aus $[A, x_1, \ldots, x_m]$ bedeuten. Mit anderen Worten: Die ganzen Größen φ_j bilden ein Fundamentalsystem.

Das demnach zu lösende Problem soll sogleich, um Wiederholungen zu vermeiden, allgemeiner formuliert werden.

Es seien $\varphi_1, \varphi_2, \ldots, \varphi_k$ wirkliche ganze Größen des dem Gattungsbereiche (Γ) zugehörigen Galoisschen Bereichs, P eine Primform des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ und weiter (nach § 12, Satz III):

$$P = (\mathfrak{p}\mathfrak{q}\mathfrak{r}\ldots)^a;$$

es sollen dann die gleichfalls dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehörigen Formen $X_1, \ldots, X_k$ in allgemeinster Weise so bestimmt werden, daß

$$X_1\varphi_1 + \cdots + X_k\varphi_k \equiv 0 \pmod{\mathfrak{p}^c\mathfrak{q}^c\mathfrak{r}^c\cdots}, \qquad (C)$$

wo $c = 1, 2, \ldots, a$ sein kann.

Dabei zeigt sich vor allem, daß mit dem Falle $c = 1$ auch die übrigen Fälle $c > 1$ vollständig erledigt sind. Ist nämlich — wie nachher nachgewiesen werden soll — die allgemeine Lösung der Kongruenz

$$X_1\varphi_1 + \cdots + X_k\varphi_k \equiv 0 \pmod{\mathfrak{p}\mathfrak{q}\mathfrak{r}\cdots}$$

in der Gestalt

$$X_i = H_{i1}\,Y_1 + \cdots + H_{il}\,Y_l$$

gegeben, so müssen auch die Lösungen der Kongruenz (C) diese Gestalt haben und die Größen X_i genügen gewiß auch dieser Kongruenz (C), wenn weiter

$$Y_1\sum_{i=1}^{k} H_{i1}\varphi_i + \cdots + Y_l\sum_{i=1}^{k} H_{il}\varphi_i \equiv 0 \pmod{\mathfrak{p}^c\mathfrak{q}^c\mathfrak{r}^c\cdots} \qquad (C')$$

ist. Nun ist aber ihrer Entstehung nach jede der Größen $\sum_{i=1}^{k} H_{ij}\varphi_i$ durch $\mathfrak{p}\mathfrak{q}\mathfrak{r}\ldots$ teilbar, und der größte gemeinschaftliche Teiler dieser Größen, ihrer sämtlichen konjugierten und P genau eine Potenz von $\mathfrak{p}\mathfrak{q}\mathfrak{r}$. Wäre nämlich für irgend eine dieser Größen

$$\left(\sum_{i=1}^{k} H_{ij}\varphi_i^{(e)},\ P\right) \sim \mathfrak{p}^r\mathfrak{q}^s\ldots,$$

so wäre, da die verbundenen Primideale in einem Galoisschen Bereiche auch konjugierte Ideale sind, für irgend eine konjugierte Größe auch

$$\left(\sum_{i=1}^{k} H_{ij}\varphi_i^{(\nu)},\ P\right) \sim \mathfrak{p}^s \mathfrak{q}^t \ldots,$$

und im größten gemeinschaftlichen Teiler aller dieser Größen muß demnach der Exponent des Primideals $\mathfrak{p}$ die kleinste aller Zahlen sein, die als Exponenten überhaupt vorkommen.

Es ist demnach

$$\mathfrak{d} \sim \left(\sum_{i=1}^{k} H_{i1}\varphi_i^{(1)}, \ldots,\ \sum_{i=1}^{k} H_{i1}\varphi_i^{(N)}, \ldots,\ P\right) \sim \mathfrak{p}^g \mathfrak{q}^g \ldots,$$

wo $g \leqq a$ sein muß.

Die Kongruenz (C′) kann also, wenn wir den Teiler $\mathfrak{d}$ entfernen, auch in der Gestalt

$$Y_1 \frac{\sum_{i=1}^{k} H_{i1}\varphi_i}{\mathfrak{d}} + \cdots + Y_l \frac{\sum_{i=1}^{k} H_{il}\varphi_i}{\mathfrak{d}} \equiv 0 \ (\text{mod. } \mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots) \quad (C'')$$

geschrieben werden*).

Dabei sei sogleich auf den wichtigen Umstand aufmerksam gemacht, daß die Bestimmung der Größe $\mathfrak{d}$ die Kenntnis der Zerlegung von P in seine Primideale nicht voraussetzt; und ferner, daß, wenn der Modul der Kongruenz (C′) ohne diese Zerlegung bekannt ist, dies auch für

*) Daß wir hier in der Kongruenz durch $\mathfrak{d}$ wirklich dividieren können, obgleich keine bloße Äquivalenzbestimmung stattfindet, ist eine Folge davon, daß $\mathfrak{d}$ nicht bloß als Ideal im Sinne der Äquivalenzbestimmung betrachtet wird, sondern als einem holoiden Bereiche angehörige Größe im vollen Sinne dieses Wortes gegeben ist. Dies könnte weder in Dedekinds noch in Kroneckers Theorie geschehn und konstituiert jene — eben durch diese und andere Anwendungen wichtige — Erweiterung der Theorie der idealen Größen, auf welche schon in § 8 hingewiesen wurde und die — in dieser Darstellung zum ersten Male — einen definitiven Abschluß der hierher gehörigen arithmetischen Grundprobleme gestattet.

den Modul der Kongruenz (C″) der Fall ist, da ja nur aus $(\mathfrak{p}\mathfrak{q}\mathfrak{r}\ldots)^c$ der Teiler $\mathfrak{d}$ zu entfernen ist.

Die linke Seite der Kongruenz (C″) wird, wenn man die Division durch $\mathfrak{d}$ nach den früher für die idealen Größen festgesetzten Rechnungsregeln wirklich ausführt, ein Quotient zweier Formen, in denen als Unbestimmte vorerst die bei der tatsächlichen Bildung von $\mathfrak{d}$ auftretenden neuen Unbestimmten zu betrachten sind. Die im Nenner auftretende Form ist primitiv und kann demnach in der Kongruenz, da wir damit nur zu einer äquivalenten idealen Größe übergehn, ganz weggelassen werden. Jener Zähler endlich wird dann und nur dann durch $\mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots$ teilbar, wenn dies für jeden Koeffizienten in der nach den Potenzprodukten der neuen Unbestimmten geordneten Form der Fall ist.

Man erhält demnach zur Bestimmung der Y das mit der Kongruenz (C′) oder (C″) gleichwertige Kongruenzensystem:

$$Y_1 \Psi_{1r} + Y_2 \Psi_{2r} + \cdots + Y_s \Psi_{sr} \equiv 0 \pmod{\mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots} \qquad (r = 1, 2\ldots) \qquad (C''')$$

und damit die gesuchte Reduktion des Problems, da der Modul jetzt eine niedrigere Potenz von $\mathfrak{p}\mathfrak{q}\ldots$ ist als früher. Daß dabei statt einer Kongruenz nun ein System von solchen Kongruenzen auftritt, ist unwesentlich. Ist nämlich die allgemeine Auflösung einer solchen Kongruenz bekannt und insbesondere in der vorausgesetzten Gestalt einer endlichen Schar gegeben, so wird diese in den übrigen einzusetzen sein. Dadurch wird die Aufgabe weiter auf ein System reduziert, in dem die Anzahl der Kongruenzen sich um Eins verringert hat, eventuell auch um mehrere, wenn unter den resultierenden Kongruenzen sich auch solche finden, die identisch befriedigt sind.

Diese Reduktionsmethode muß aber immer nach einer endlichen Anzahl von Schritten zu einem Systeme identisch befriedigter Kongruenzen führen, in denen jeder Koeffizient durch $\mathfrak{p}^{c-g}\mathfrak{q}^{c-g}\ldots$ teilbar ist, also die Y sich als keiner weiteren Bedingung unterworfene beliebige Formen bestimmen. Da nämlich bei jedem einzelnen Schritte dieses Verfahrens

der gemeinsame Exponent der Primideale $\mathfrak{p}, \mathfrak{q}, \ldots$ sich wenigstens um Eins erniedrigt, muß dies, wenn nicht früher, so doch nach c Schritten geschehn, wo dann der Modul ~ 1 geworden ist. Ob und wann dies geschehe, ersieht man unmittelbar durch Bildung der Größe

$$\mathrm{Nm.}\frac{\mathfrak{p}^c\mathfrak{q}^c\ldots}{\mathfrak{d}},$$

die dann als Quotient primitiver Formen erscheint.

Wie schon hervorgehoben wurde, setzt das Verfahren die Kenntnis der Zerlegung von P in Primideale nicht voraus, nur muß der Modul $\mathfrak{p}^c\mathfrak{q}^c\ldots$ irgendwie gegeben sein. Jene Zerlegung von P ist nur als theoretisches Hilfsmittel für die Begründung des Verfahrens benutzt, gelangt aber bei der praktischen Ausführung nicht zur Anwendung. Es genügt daher der für diese Zerlegung früher gegebene Existenzbeweis, und es wird umgekehrt die jetzt entwickelte Methode durch die damit gegebene Herstellung des Fundamentalsystems dahin führen, daß wir auch die Zerlegung von P in Primideale tatsächlich ausführen.

Das zu Beginn dieses Paragraphen formulierte Problem verlangt nun geradezu die Auflösung der Kongruenz

$$X_1\varphi_1 + \cdots + X_k\varphi_k \equiv 0 \pmod{P};$$

dabei ist P jedenfalls eine genaue Potenz von $\mathfrak{p}\mathfrak{q}\ldots$, und es trifft auch die weitere früher betonte Voraussetzung ein, daß der Modul der Kongruenz eine tatsächlich gegebene Größe ist. Das ganze Verfahren, dessen wir zur Aufstellung des Fundamentalsystems irgend eines Gattungsbereichs benötigen, ist demnach auf die Auflösung der Kongruenz

$$X_1\varphi_1 + \cdots + X_k\varphi_k \equiv 0 \pmod{\mathfrak{p}\mathfrak{q}\ldots}$$

zurückgeführt, wo $\mathfrak{p}, \mathfrak{q}, \ldots$ die verschiedenen in P enthaltenen Primgrößen bedeuten; das Verfahren zur Auflösung jener Kongruenz wird aber wieder unabhängig von der Kenntnis der Zerlegung von P zu formulieren sein.

§ 22. Um das auf seine einfachste Gestalt gebrachte Problem zu erledigen, bilde man

$$F = \Pi(z - \varphi_1^{(i)} z_1 - \cdots - \varphi_k^{(i)} z_k),$$

wo das Produkt auf die verschiedenen konjugierten Werte von $z - \varphi_1 z_1 - \cdots - \varphi_k z_k$ zu erstrecken ist und also F eine dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form der neuen Unbestimmten $z, z_1, \ldots, z_k$ ist. Wird das Produkt nach dem Äquivalenzmodul P in irreduzible Faktoren zerlegt, so ergibt sich:

$$F \sim F_1^{a_1} F_2^{a_2} \ldots \text{ (aequ. mod. } P).$$

Diese Äquivalenz ist, wie wir wissen, mit einer Kongruenz

$$Q' F \equiv Q'' F_1^{a_1} F_2^{a_2} \ldots \text{ (mod. } P)$$

gleichbedeutend, wo Q' und Q'' dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehörige, zu P teilerfremde Größen sind. Der zu Grunde gelegte Galoissche Bereich werde weiter durch Adjunktion sämtlicher Wurzeln der Gleichung

$$F F_1 F_2 \ldots = 0$$

erweitert, in der z als Unbekannte, $z_1, \ldots, z_k$ auch weiterhin als Unbestimmte zu fassen sind. Die Wurzeln der Gleichung $F = 0$ sind dann die konjugierten Größen $\varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k$.

Die Wurzeln der Gleichungen $F_1 = 0$, $F_2 = 0, \ldots$ mögen endlich mit

$$\alpha_1, \ldots, \alpha_{l_1}; \beta_1, \ldots, \beta_{l_2}; \ldots$$

bezeichnet werden, wo demnach $l_1, l_2, \ldots$ den Grad von $F_1, F_2, \ldots$ in z bezeichnen; es ist dann noch, wenn F in z vom Grade l ist:

$$l = a_1 l_1 + a_2 l_2 + \cdots$$

Ist nun $\mathfrak{p}$ irgend ein in P enthaltenes Primideal, so besteht auch die Kongruenz

$$Q' F \equiv Q'' F_1^{a_1} F_2^{a_2} \ldots \text{ (mod. } \mathfrak{p}),$$

und es müssen die Größen

$$\varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k$$

einerseits und die Größen

$$\alpha_1, \ldots, \alpha_{l_1};\ \beta_1, \ldots, \beta_{l_2};\ \ldots$$

andrerseits, wenn jedes α a_1-mal, jedes β a_2-mal u. s. f. gezählt wird, abgesehn von der Reihenfolge mod. $\mathfrak{p}$ übereinstimmen*). Die Größen $\alpha_1, \ldots, \alpha_{l_1};\ \beta_1, \ldots, \beta_{l_2}$ sind dabei mod. $\mathfrak{p}$ durchweg verschieden; im entgegengesetzten Falle müßte die Discriminante irgend eines F_i, oder die Resultante zweier solcher Formen F_i, F_j nach dem Modul $\mathfrak{p}$ oder, da dies Formen der z sind, die dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammen, auch mod. P verschwinden. Dies ist aber nach ihrer Bildung und dem Satze in § 20 ausgeschlossen.

Allerdings scheinen diese Entwicklungen, insbesondere auch die in der Fußnote gegebene Schlußweise an die Voraussetzung geknüpft, daß die $\alpha, \beta, \ldots$ ganze Größen sind. Dies ist im allgemeinen durchaus nicht der Fall, insbesondere nicht, wenn der Äquivalenzmodul P die Unbestimmten $x_1, \ldots$ enthält. Dann ist der Koeffizient der höchsten Potenz von z in $F_1, F_2, \ldots$ durchaus nicht 1, sondern, weil F eine reguläre Form der z ist, eine Form des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$, von der nur feststeht, daß sie zu P teilerfremd ist.

Demnach wird, wenn A der Koeffizient der höchsten Potenz von z in F ist, nicht α, wohl aber $A\alpha = \alpha'$ eine ganze Größe. Man kann aber, wie dies auch häufig in den Elementen der Zahlentheorie geschieht, anstandslos in den Kongruenzen mod. $\mathfrak{p}$ solche Größen zulassen, deren Nenner

---

*) Ist nämlich

$$Q'(z-\mu_1)(z-\mu_2)\ldots \equiv Q''(z-\nu_1)(z-\nu_2)\ldots \pmod{\mathfrak{p}},$$

so muß

$$Q'(\nu_1-\mu_1)(\nu_1-\mu_2)\ldots \equiv 0 \pmod{\mathfrak{p}}$$

sein. Da ferner (Q', P) und also auch $(Q', \mathfrak{p}) \sim 1$, muß ferner, weil $\mathfrak{p}$ ein Primideal ist, einer der Faktoren durch $\mathfrak{p}$ teilbar sein. Ist dies z. B. $\nu_1 - \mu_1$, also $\nu_1 \equiv \mu_1 \pmod{\mathfrak{p}}$, so kann man den Faktor $z - \mu_1 \equiv z - \nu_1$ auf beiden Seiten entfernen und erhält also wieder z. B. $\nu_2 \equiv \mu_2 \pmod{\mathfrak{p}}$ u. s. f. Für diesen Schluß ist nur zu beachten, daß das gewöhnliche Divisionsverfahren nach einem Primmodul eindeutig bestimmt ist.

durch $\mathfrak{p}$ nicht teilbar ist, wenn man die Kongruenzbeziehung

$$\frac{\mu}{A} \equiv \frac{\nu}{B} \pmod{\mathfrak{p}}$$

einfach als andere Schreibweise für

$$B\mu \equiv A\nu \pmod{\mathfrak{p}}$$

betrachtet. So hat dann die Kongruenz

$$\alpha \equiv \varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k \pmod{\mathfrak{p}}$$

die folgende Bedeutung

$$A\alpha \equiv \alpha' \equiv A(\varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k) \pmod{\mathfrak{p}}.$$

Die in der vorstehenden Fußnote gegebene Schlußweise ist leicht auf den Fall zu übertragen, wo $\mu_1, \mu_2, \ldots, \nu_1, \nu_2, \ldots$ nicht ganz sind, dies aber für $A_1\mu_1, A_2\mu_2, \ldots, B_1\nu_1, B_2\nu_2, \ldots$ der Fall ist, wo $A_1, A_2, \ldots, B_1, B_2, \ldots$ durch $\mathfrak{p}$ nicht teilbare Größen sind. (Man bemerke dabei noch, daß dann die A und B auch zu P teilerfremd sind, also auch durch die verbundenen oder konjugierten Primideale $\mathfrak{q}, \mathfrak{r}, \ldots$ nicht teilbar sind.) Es ist dann nur mehr $A_1 A_2 \ldots B_1 B_2 \ldots z = z'$ durch Multiplikation mit der entsprechenden Potenz von $A_1 A_2 \ldots B_1 B_2$ einzuführen.

§ 23. Wenn wir nach diesen weiteren Festsetzungen zu der von Anfang des vorstehenden Paragraphen entwickelten Kongruenz zurückkehren, so hat man endlich in

$$F_1 F_2 \ldots \equiv 0 \pmod{\mathfrak{p}}$$

eine Kongruenz, deren Wurzeln die mod. $\mathfrak{p}$ verschiedenen Größen

$$\varphi_1^{(i)} z_1 + \cdots + \varphi_k^{(i)} z_k$$

sind, wobei die Anzahl der Wurzeln mit dem Grade dieser Kongruenz, $l_1 + l_2 + \cdots$, übereinstimmt. Ist der Koeffizient der höchsten Potenz von z in dieser Kongruenz gleich Q, so ist Q eine zu P teilerfremde Form des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$, und man hat endlich, wenn man der Kürze wegen

$$\Phi = F_1 F_2 \ldots$$

setzt (ähnlich wie in Kap. VI. § 15):

$$\left[\frac{\partial \Phi}{\partial z}\right]_{z=\Sigma \varphi_r^{(i)} z_r} \varphi_r^{(i)} + \left[\frac{\partial \Phi}{\partial z_r}\right]_{z=\Sigma \varphi_r^{(i)} z_r} \equiv 0 \pmod{\mathfrak{p}}.$$

Nun ist die Discriminante von Φ nach z eine Form aus $[\mathsf{A}, x_1, \ldots, x_m, z_1, z_2, \ldots]$, die mod. P von Null verschieden ist, und behält diese Eigenschaft, wenn man für $z_1, z_2, \ldots$ entsprechend gewählte, leicht zu bestimmende Größen $Z_1, Z_2, \ldots$ aus $[\mathsf{A}, x_1, \ldots, x_m]$ setzt*).

Bezeichnet man die Ausführung der Substitution

$$z = \Sigma \varphi_r^{(i)} Z_r,\ z_r = Z_r$$

kurz mit $[\ldots]_{Z^{(i)}}$, so wird

$$\left[\frac{\partial \Phi}{\partial z}\right]_{Z^{(i)}}$$

mod. $\mathfrak{p}$ von Null verschieden, und es wird auch das über die mod. $\mathfrak{p}$ verschiedenen $l_1 + l_2 + \cdots$ Größensysteme $\varphi_1^{(i)} \ldots \varphi_k^{(i)}$ erstreckte Produkt

$$\Pi \left[\frac{\partial \Phi}{\partial z}\right]_{Z^{(i)}}$$

von Null mod. $\mathfrak{p}$ verschieden sein. Es entsteht aus

$$\Pi \left[\frac{\partial \Phi}{\partial z}\right]_{z=\Sigma \varphi_r^{(i)} z_r},$$

wenn man $z_r = Z_r$ setzt; diese Größe ist eine symmetrische Form der Wurzeln von $\Phi \equiv 0 \pmod{\mathfrak{p}}$, und also mod. $\mathfrak{p}$

*) Für diese Schlußweise ist es wieder (ebenso, wie in Kap. VIII. § 4) nur notwendig, daß es unendlich viele mod. P von einander verschiedene Größen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ gebe. Dies ist immer der Fall, wenn der Bereich Unbestimmte enthält. Ist P eine gewöhnliche Primzahl, so sind $1, x_1, x_1^2, \ldots$ solche Größen; enthält P zumindest eine Unbestimmte, so sind $1, 2, 3, \ldots$ Größen der gesuchten Art. Ausgeschlossen bleibt nur der Fall der algebraischen Zahlen, wo an Stelle von $[\mathsf{A}, x_1, \ldots, x_m]$ der Bereich $[1]$ tritt. Dann ist der anzuwendende Schluß allerdings eventuell falsch, und ebendeshalb mußte das hier allgemein zu lösende Problem gerade für diesen allereinfachsten Grenzfall früher gesondert betrachtet (und erledigt) werden.

nach Multiplikation mit einer genügend hohen Potenz von Q als Form S aus $[\mathsf{A}, x_1, \ldots, x_m, z_1, z_2, \ldots]$ darstellbar, die mod. P von Null verschieden ist.

Ganz ähnlich sieht man, daß das Produkt

$$\Pi^{(i)}\left[\frac{\partial \Phi}{\partial z}\right]_{z^{(j)}},$$

wo gerade der Faktor $\left[\frac{\partial \Phi}{\partial z}\right]_{z^{(i)}}$ auszuschließen ist, aus

$$\Pi^{(i)}\left[\frac{\partial \Phi}{\partial z}\right]_{z=\Sigma \varphi_r^{(j)} z_r}$$

durch die Substitution $z_r = Z_r$ entsteht. Diese letzte Größe ist symmetrisch in Bezug auf die Größen $\Sigma \varphi_r^{(j)} z_r$ mit Ausschluß von $\Sigma \varphi_r^{(i)} z_r$, also mod. $\mathfrak{p}$ nach Multiplikation mit einer genügend hohen Potenz von Q in der Gestalt

$$[\Psi(z, z_1, z_2, \ldots]_{z=\Sigma \varphi_r^{(i)} z_r}$$

darstellbar, und es ergibt sich endlich

$$S \varphi_r^{(i)} \equiv \left[- \Psi \frac{\partial \Phi}{\partial z_r}\right]_{z^{(i)}} \pmod{\mathfrak{p}},$$

oder

$$\bar{S} \varphi_r^{(i)} \equiv \psi_r(\xi_i, Z_1, Z_2, \ldots) \pmod{\mathfrak{p}},$$

wo $\xi_1, \xi_2, \ldots$ der Reihe nach die Wurzeln der Kongruenz

$$[F_1 F_2 \ldots]_{z_r = Z_r} \equiv 0 \pmod{\mathfrak{p}},$$

d. h. die Größen $\varphi_1^{(i)} Z_1 + \cdots + \varphi_k^{(i)} Z_k$ bezeichnen. Diese Kongruenz besitzt, da die Z_r entsprechend gewählt sind, auch jetzt so viele (mod. $\mathfrak{p}$) verschiedene Wurzeln, als ihr Grad Einheiten zählt, und jeder ihrer Wurzeln ξ_i entspricht ein Größensystem $\varphi_1^{(i)}, \varphi_2^{(i)}, \ldots$. Dabei ist diese Bestimmung der Größen $\varphi_r^{(i)}$ bei jeder Wahl des in P enthaltenen Primideals dieselbe; und es kann, wenn die Rechnung statt auf $\mathfrak{p}$ nun auf $\mathfrak{q}$ bezogen wird, eine Verschiedenheit nur insofern eintreten, als die konjugierten Größen $\varphi_r^{(i)}$ in andrer Reihenfolge auftreten.

Mit der Kongruenz

$$X_1 \varphi_1 + \cdots + X_k \varphi_k \equiv 0 \pmod{\mathfrak{p}\,\mathfrak{q}\ldots}$$

ist das System von Kongruenzen

$$X_1 \varphi_1^{(i)} + \cdots + X_k \varphi_k^{(i)} \equiv 0 \pmod{\mathfrak{p}\,\mathfrak{q}\cdots} \qquad (i = 1, 2, \cdots)$$

gleichbedeutend; und für dieses kann wieder

$$\begin{aligned} X_1 \varphi_1^{(i)} + \cdots + X_k \varphi_k^{(i)} &\equiv 0 \pmod{\mathfrak{p}} \qquad (i = 1, 2, \cdots) \\ X_1 \varphi_1^{(i)} + \cdots + X_k \varphi_k^{(i)} &\equiv 0 \pmod{\mathfrak{q}} \qquad (i = 1, 2, \cdots) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

gesetzt werden, da ja $\mathfrak{p}$, $\mathfrak{q}$, ... verschiedene Primideale sind.

Irgend eines, z. B. das erste dieser Systeme, geht durch Multiplikation mit $\bar{S}$ in

$$X_1 \psi_1(\xi_i) + \cdots + X_k \psi_k(\xi_i) \equiv 0 \pmod{\mathfrak{p}} \qquad (i = 1, 2, \cdots)$$

über, und dieses System kann wieder durch das völlig gleichbedeutende System

$$\sum_{(i)} \xi_i^r (X_1 \psi_1(\xi_i) + \cdots + X_k \psi_k(\xi_i)) \equiv 0 \pmod{\mathfrak{p}} \qquad (r = 1, 2, \cdots)$$

ersetzt werden. (Daß auch hier erst die Größen $Q\xi_i$ ganz sind, man also wieder mit einer Potenz von Q multiplizieren muß, um Kongruenzen im engeren Sinne des Wortes zu erhalten, d. h. Eigenschaften von ganzen Größen auszudrücken, braucht wohl nicht mehr besonders hervorgehoben zu werden.) Das letztere System ersetzt das vorstehende vollständig, weil ja $|\xi_i^r|^2$, wieder mit einer Potenz von Q multipliziert, eine zu $\mathfrak{p}$ teilerfremde ganze Größe ist.

Nun hat man auf der linken Seite in jeder Kongruenz des letzten Systems eine symmetrische Form der ξ_i, und dieses geht daher in die rationale und ganze Gestalt

$$A_{1r} X_1 + \cdots + A_{kr} X_k \equiv 0 \pmod{P} \qquad (r = 1, 2, \cdots)$$

über; denn eine durch $\mathfrak{p}$ teilbare Form aus $[\mathsf{A}, x_1, \ldots, x_m]$ ist stets auch durch P teilbar und umgekehrt. Das ist aber ein System von linearen diophantischen Gleichungen im Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$, und hieraus ergibt sich in bekannter Weise die allgemeine Lösung, und zwar, wie behauptet in Gestalt einer endlichen Schar.

Da endlich von $\mathfrak{p}$ nur eben vorausgesetzt wurde, daß dieses Ideal ein in P enthaltenes Primideal ist, bezieht sich die erhaltene Lösung genau ebenso auch auf $\mathfrak{q}$, $\mathfrak{r}$, ... und ist also auch die allgemeine Lösung der Kongruenz

$$X_k \varphi_1 + \cdots + X_k \varphi_k \equiv 0 \pmod{\mathfrak{p}\mathfrak{q}\cdots}.$$

Damit sind wir aber im Besitze aller Hilfsmittel, um das Fundamentalsystem der wirklichen ganzen Größen eines beliebigen Gattungsbereiches durch eine endliche Anzahl bekannter Operationen wirklich zu berechnen.

Daß die tatsächliche Lösung eines so allgemeinen, in die verschiedensten Disziplinen der Mathematik hineinragenden Problems sich rechnerisch langwierig gestalten muß, war wohl vorauszusehn. Doch wird der volle Überblick der allgemeinen Arithmetik der algebraischen Größen uns lehren, daß die hier gegebene Methode, gerade weil sie mit der Zerlegung gewisser rationaler und ganzer Größen in Primideale parallel läuft, die einzige naturgemäße Methode ist, die, ohne der Natur der Sache fremde Hilfsmittel zu verwenden, die wesentlichen Eigenschaften der zu untersuchenden arithmetisch-algebraischen Gebilde prinzipiell klarstellt.

Das Fundamentalsystem der idealen Größen eines Gattungsbereichs.

§ 24. Ist $\mu_1, \mu_2, \ldots, \mu_r$ ein Fundamentalsystem der wirklichen ganzen Größen des Gattungsbereichs (Γ), so kann dieses in gewissem Sinne auch als Fundamentalsystem der idealen ganzen Größen desselben Gattungsbereichs angesehn werden. Jede solche ideale ganze Größe kann, wenn sie als Quotient zweier dem Gattungsbereiche entstammender ganzer algebraischer Formen definiert wird, unmittelbar so geschrieben werden, daß der Nenner „in Bezug auf $[\mathsf{A}, x_1, \ldots, x_m]$“ auch rational und ganz ist, d. h. so, daß dieser Nenner eine dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende, primitive Form wird. Ist die ganze ideale Größe in dieser Weise geschrieben:

$$\mathfrak{a} = \frac{\alpha_0 U_{k_0} + \alpha_1 U_{k_1} + \cdots}{\varepsilon},$$

so kann jeder Koeffizient α_i als wirkliche ganze Größe aus $[\Gamma]$ mit Hilfe des Fundamentalsystems auf die Gestalt

$$\alpha_i = a_{i1}\mu_1 + a_{i2}\mu_2 + \cdots + a_{ir}\mu_r$$

gebracht werden, wo die Größen a Formen aus $[\mathsf{A}, x_1, \ldots, x_m]$ sind; ordnet man also nach den Größen μ, so wird

$$\mathfrak{a} = \mathfrak{k}_1\mu_1 + \mathfrak{k}_2\mu_2 + \cdots + \mathfrak{k}_r\mu_r,$$

wo die $\mathfrak{k}$ rationale und ganze ideale Größen sind, d. h. durch Quotienten zweier aus $[\mathsf{A}, x_1, \ldots, x_m]$ entstammenden Formen — selbstverständlich mit primitivem Nenner — dargestellt werden.

Diese Darstellung der ganzen idealen Größen eines Gattungsbereichs gestattet aber noch eine wesentliche Vereinfachung, die von ganz neuen Gesichtspunkten aus wieder zeigt, wie sehr die Association der idealen Größen bei der Untersuchung eines Gattungsbereichs naturgemäß und zweckdienlich ist.

Während nämlich die Anzahl der Elemente, die in ein Fundamentalsystem der wirklichen Größen des Gattungsbereichs aufgenommen werden müssen, im allgemeinen größer ist als die Ordnungszahl des Gattungsbereichs, gibt es nach Association der idealen Größen immer Fundamentalsysteme von n Elementen, wenn n die Ordnung der Gattung bezeichnet, wo aber in gewissen Fällen die Bezeichnung als Fundamentalsystem etwas allgemeiner als bisher zu verstehen ist. Ausführlicher formuliert, gibt es immer n ideale ganze Größen $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ von der Beschaffenheit, daß jede ideale ganze Größe des Gattungsbereichs als homogene und lineare Form von $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ darstellbar ist, und zwar so, daß die Koeffizienten rationale und ganze ideale Größen des Gattungsbereichs werden, wenn wir sie mit einer bestimmten — später vollständig zu berechnenden — rationalen und ganzen Zahl d multiplizieren.

Dieses Fundamentalsystem der idealen ganzen Größen ist aus dem Fundamentalsysteme der wirklichen ganzen Größen ohne jede weitere Rechnung herzustellen. Ist nämlich $\mu_1, \ldots, \mu_r$ das letztere Fundamentalsystem, sind ferner die $u_1, \ldots, u_r$ neue Unbestimmte, und

$$\mathfrak{g} = \mu_1 u_1 + \cdots + \mu_r u_r,$$

so ist in der soeben auseinandergesetzten Bedeutung

$$1, \mathfrak{g}, \mathfrak{g}^2, \ldots, \mathfrak{g}^{n-1}$$

das Fundamentalsystem der idealen ganzen Größen des Gattungsbereichs*).

Bevor wir jedoch an die Begründung dieses wesentlichsten Fundamentalsatzes der allgemeinen Arithmetik gehn, muß noch eine Reihe einfacher Bemerkungen vorausgeschickt werden.

Die Größe $\mathfrak{g}$ soll in der Folge als Fundamentalgröße oder Fundamentalform der Gattung bezeichnet werden. Ihrer Bildung nach stellt sie, wenn für $u_1, \ldots, u_r$ beliebige Formen aus $[A, x_1, \ldots, x_m]$ und nur diese zugelassen werden, alle wirklichen ganzen Größen des Gattungsbereichs dar. Man sieht unmittelbar, daß $\mathfrak{g}$ eine Einheit ist. Denn es ist $\mathfrak{g}$ der größte gemeinschaftliche Teiler von $\mu_1, \ldots, \mu_r$, und dieser muß, da auch eine Gleichung

$$1 = \mu_1 c_1 + \cdots + \mu_r c_r$$

besteht, ein Teiler der Eins sein.

---

*) Durch Einführung der hier benutzten, auch dem gewöhnlichen Additionsgesetze unterworfenen idealen Größen wird Fassung und Beweis des hier vorgetragenen Satzes besonders einfach. Die entsprechenden Erörterungen der Kroneckerschen Festschrift finden sich in § 25.

Selbstverständlich bezieht sich die Frage, ob es wirklich notwendig ist, einen Faktor d hinzuzufügen, nur auf die Untersuchung der absolut ganzen Größen; da im Falle relativ ganzer Größen jede gewöhnliche rationale Zahl als der Einheit äquivalent zu betrachten ist.

Für den Fall $[A, x_1, \ldots, x_m] = [1]$, d. h. für die Theorie der algebraischen Zahlen hat K. Hensel diese Fragen durch elegante, spezielle Methoden endgültig erledigt. („Untersuchung der Fundamentalgleichung einer Gattung etc." Journal f. r. u. a. Math. Bd. 113, 1893.)

Es ist $\mathfrak{g}$ eine Größe n^{ter} Ordnung; denn die Gleichung

$$\text{Nm.}(z - \mathfrak{g}) = 0,$$

der sie genügt, muß irreduzibel sein, da dies auch bei jenen Werten der u stattfindet, für welche $\mathfrak{g}$ eine wirkliche ganze Größe n^{ter} Ordnung wird. Die n konjugierten Größen $\mathfrak{g}_1, \ldots, \mathfrak{g}_n$ sind demnach sämtlich verschieden.

Die Gleichung

$$\text{Nm.}(z - \mathfrak{g}) = 0,$$

die in gewisser Weise alle ganzen Größen des Gattungsbereichs — wirkliche und ideale — umfaßt, soll als Fundamentalgleichung der Gattung bezeichnet werden.

Die Discriminante der Fundamentalgleichung, $\mathfrak{D}$, ist unmittelbar bekannt und kann

$$\mathfrak{D} = P_1 \ldots P_r E$$

geschrieben werden, wo $P_1, \ldots, P_r$ gleiche oder verschiedene Primformen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ bedeuten, und E eine diesem Bereiche entstammende primitive Form der u ist. Man hat also:

$$\mathfrak{D} \sim P_1 \ldots P_r.$$

Soll nun für irgend eine ideale ganze Größe $\mathfrak{a}$ eine Identität von der Gestalt

$$\mathfrak{a} = \mathfrak{r}_0 + \mathfrak{r}_1 \mathfrak{g} + \cdots + \mathfrak{r}_{n-1} \mathfrak{g}^{n-1}$$

stattfinden, wo die $\mathfrak{r}$ rationale ideale Größen sind, so muß diese Identität in den n konjugierten Gattungsbereichen in gleicher Weise gelten. Sind also die n konjugierten Werte von $\mathfrak{a}$ der Reihe nach $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, so sind die $\mathfrak{r}$ durch die Bedingungen

$$\mathfrak{a}_i = \mathfrak{r}_0 + \mathfrak{r}_1 \mathfrak{g}_i + \cdots + \mathfrak{r}_{n-1} \mathfrak{g}_i^{n-1}$$
$$(i = 1, 2, \ldots, n)$$

gegeben, und es ergibt sich für die Größen $\mathfrak{r}$ eine eindeutige Bestimmung von der Gestalt:

$$\mathfrak{r}_j = \frac{\mathfrak{k}_j}{\mathfrak{D}},$$

wo die Größen $\mathfrak{k}_j$, weil die $\mathfrak{a}_i$ ganz sind, rationale und ganze ideale Größen sind.

Der zu beweisende Satz besagt nun, daß die so bestimmten Größen $d\mathfrak{k}_j$, wie immer auch die ganze Größe $\mathfrak{a}$ gewählt sei, immer durch $\mathfrak{D}$ teilbar sind, und kann also auch folgendermaßen ausgesprochen werden: Eine ganze ideale Größe der Gestalt $\mathfrak{k}_0\mathfrak{g}^{n-1} + \mathfrak{k}_1\mathfrak{g}^{n-2} + \cdots + \mathfrak{k}_{n-1}$ kann nur dann durch $\mathfrak{D}$ teilbar sein, wenn jede der rationalen und ganzen idealen Größen $d\mathfrak{k}_0$, $d\mathfrak{k}_1$, ... durch $\mathfrak{D}$ teilbar ist.

§ 25. Der soeben ausgesprochene Satz ist, wie man unmittelbar sieht, in dem folgenden einerseits einfacheren, andrerseits allgemeineren Satze enthalten:

Sind $\mathfrak{k}_0, \ldots, \mathfrak{k}_{n-1}$ rationale und ganze ideale Größen, $\mathfrak{g}$ die Fundamentalgröße des Gattungsbereichs, so kann $\mathfrak{k}_0\mathfrak{g}^{n-1} + \mathfrak{k}_1\mathfrak{g}^{n-2} + \cdots + \mathfrak{k}_{n-1}$ nur dann durch irgend eine Primform P des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ teilbar sein, wenn jede der Größen $d_P\mathfrak{k}_0$, $d_P\mathfrak{k}_1$, ... diese Eigenschaft besitzt.

Für den Fall relativ ganzer Größen ist $d = 1$ zu nehmen; ebenso in der Theorie der absolut ganzen Größen für jede wirkliche Primform, sowie für jede natürliche Primzahl p, die nicht zugleich in $(n-2)!$ und der Discriminante der Fundamentalgleichung als Teiler enthalten ist. Ist in letzterem Falle $\mathfrak{D}$ genau durch p^a teilbar, so genügt es jedenfalls $d_p = p^{e\left(\frac{a}{2}\right)}$ zu nehmen, wo $e\left(\frac{a}{2}\right)$ die größte in $\frac{a}{2}$ enthaltene ganze Zahl bedeutet.

Das Prinzip des Beweises rührt von Kronecker*) her.

Jede ganze ideale Größe des Bereichs $\mathfrak{a}$ kann in der Gestalt $\mathfrak{h}_1\mu_1 + \mathfrak{h}_2\mu_2 + \cdots + \mathfrak{h}_r\mu_r$ geschrieben werden. Dann hat man für die Differenz zweier konjugierter Werte $\mathfrak{a}_i$ und $\mathfrak{a}_j$:

$$\mathfrak{a}_i - \mathfrak{a}_j = \mathfrak{h}_1(\mu_{1i} - \mu_{1j}) + \cdots + \mathfrak{h}_r(\mu_{ri} - \mu_{rj}).$$

*) Festschrift, § 25.

Die Differenz der entsprechenden konjugierten Werte der Fundamentalgröße ist:

$$\mathfrak{y}_i - \mathfrak{y}_j = (\mu_{1i} - \mu_{1j})\,u_1 + \cdots + (\mu_{ri} - \mu_{rj})\,u_r,$$

also nichts anderes, als der größte gemeinschaftliche Teiler der ganzen Größen $\mu_{1i} - \mu_{1j}, \ldots, \mu_{ri} - \mu_{rj}$. Hieraus folgt, daß $\mathfrak{a}_i - \mathfrak{a}_j$ immer durch $\mathfrak{y}_i - \mathfrak{y}_j$ teilbar ist*).

Ist nun $\mathfrak{k}(\mathfrak{y}) = \mathfrak{k}_0\mathfrak{y}^s + \mathfrak{k}_1\mathfrak{y}^{s-1} + \cdots + \mathfrak{k}_s$ durch P teilbar, so ist nach dem soeben gegebenen Hilfssatze auch

$$\frac{\mathfrak{k}(\mathfrak{y}_i) - \mathfrak{k}(\mathfrak{y}_j)}{P(\mathfrak{y}_i - \mathfrak{y}_j)}$$

eine ganze Größe, oder ausführlich geschrieben:

$$\sum_{h=0}^{s-2} \mathfrak{k}_h(\mathfrak{y}_i^{s-h-1} + \mathfrak{y}_j\mathfrak{y}_i^{s-h-2} + \cdots + \mathfrak{y}_j^{s-h-1}) + \mathfrak{k}_{s-1} \qquad (1)$$

durch P teilbar. Für j kann der Reihe nach jede Zahl von 1 bis n, mit Ausschluß von i, gesetzt werden. Berücksichtigt man

$$\sum_{j=1}^{n}{}^{(i)}\mathfrak{y}_j^k = S_k - \mathfrak{y}_i^k,$$

wo $S_1, \ldots, S_k$ dem Bereiche $[A, x_1, \ldots, x_m]$ entstammende Formen sind, so wird, wenn man (1) für $j = 1, \ldots, n$ mit Ausschluß von i summiert, diese Summe, die wieder eine ganze Größe und durch P teilbar ist:

$$\sum_{h=0}^{s-2} \mathfrak{k}_h((n-s+h)\mathfrak{y}_i^{s-h-1} + S_1\mathfrak{y}_i^{s-h-2} + \cdots + S_{s-h-1}) + (n-1)\mathfrak{k}_{s-1}$$

Dieser Ausdruck ist gleich

$$(n-s)\mathfrak{k}_0\mathfrak{y}_i^{s-1} + \mathfrak{k}_1'\mathfrak{y}_i^{s-2} + \cdots. \qquad (2)$$

Wendet man aber dieses Verfahren wiederholt an, so gelangt man schließlich zu dem Resultate, daß auch $(n-s)\cdots(n-2)\mathfrak{k}_0$ durch P teilbar ist; also, wenn wir in der Theorie der relativ ganzen Größen bleiben, wo jede Zahl ~ 1, endlich auch $\mathfrak{k}_0$ durch P teilbar sein muß.

*) Damit ist die Untersuchung allerdings aus dem Bereiche $[\Gamma]$ in den entsprechenden Galoisschen Bereich verlegt, was aber für die Entscheidung, ob eine Größe ganz ist, durchaus gleichgültig ist.

Für die arithmetische Theorie der absolut ganzen algebraischen Größen versagt diese Schlußweise, wenn P eine in $(n-2)!$ als Teiler enthaltene natürliche Primzahl ist.

In diesem Falle bemerke man, daß, wenn

$$\mathfrak{k}_0 \mathfrak{g}_i^s + \mathfrak{k}_1 \mathfrak{g}_i^{s-1} + \cdots + \mathfrak{k}_s$$

durch $p^{e\left(\frac{a}{2}\right)+1}$ teilbar ist und $\mathfrak{D}$ genau p^a enthält, nach elementaren Determinantensätzen $\mathfrak{k}_i^2 \mathfrak{D}$ durch $p^{2e\left(\frac{a}{2}\right)+2}$ teilbar sein muß, und also, da $a < 2e\left(\frac{a}{2}\right) + 2$ ist, $\mathfrak{k}_i^2$ oder auch $\mathfrak{k}_i$ durch p teilbar sein muß.

Damit ist nicht ausgeschlossen, daß auch für eine solche Primzahl $d = 1$ schon genügt. Insofern dies nicht stattfindet, wollen wir die betreffende Primzahl als irregulär bezeichnen. Es wäre für den Ausbau der Theorie von großem Interesse, zu entscheiden, ob solche irreguläre Primzahlen für gewisse Gattungsbereiche in der Tat existieren. Um trotz dieser Lücke den Fundamentalsatz über kritische Primformen vollständig beweisen zu können, fügen wir hier noch die folgenden Entwicklungen ein.

Es sei wieder $\mathfrak{k}(z)$ vom Grade $s \leqq n-1$ eine Form, welche die Eigenschaft besitzt, daß $\mathfrak{k}(\mathfrak{g}_i)$ durch die irreguläre Primzahl p teilbar ist, ohne daß dies für die Koeffizienten $\mathfrak{k}_0, \mathfrak{k}_1, \ldots$ stattfindet. Wir bezeichnen die Fundamentalgleichung mit $F(z) = 0$ und zerlegen sodann $F(z)$ in irreduzible Faktoren (aequ. mod. p) — oder, was hier dasselbe bedeutet, (mod. p):

$$F(z) \equiv F_1(z)^{a_1} \ldots F_r(z)^{a_r} \pmod{p}.$$

Ähnlich sei

$$\mathfrak{k}(z) \equiv F_1(z)^{b_1} \ldots F_r(z)^{b_r} G_1(z)^{c_1} \ldots \pmod{p},$$

wo, wenn $\mathfrak{k}(z) \pmod{p}$ nicht durch $F_1(z)$ teilbar ist, $b_1 = 0$ zu nehmen ist.

Setzt man jetzt $z = \mathfrak{g}_i$, so folgt, da der Annahme nach auch $\mathfrak{k}(\mathfrak{g}_i) \equiv 0 \pmod{p}$ ist:

$$F_1(\mathfrak{g}_i)^{a_1} \dots F_r(\mathfrak{g}_i)^{a_r} \equiv 0 \pmod{p}$$
$$F_1(\mathfrak{g}_i)^{b_1} \dots F_r(\mathfrak{g}_i)^{b_r} G_1(\mathfrak{g}_i)^{c_1} \dots \equiv 0 \pmod{p}.$$

Jedes Primideal von p muß also schon in einer der Größen $F_1(\mathfrak{g}_i) \dots F_r(\mathfrak{g}_i)$ als Teiler enthalten sein; und es kann demnach $G_1(\mathfrak{g}_i), \dots$ durch keines dieser Primideale teilbar sein; sonst müßte auch die Resultante von G_1 und z. B. F_j durch p teilbar sein. Da aber F_j und G_1 mod. p irreduzible und nicht äquivalente Formen sind, ist diese Resultante eine durch p nicht teilbare Größe. Es ist also schon

$$F_1(\mathfrak{g}_i)^{b_1} \dots F_r(\mathfrak{g}_i)^{b_r} \equiv 0 \pmod{p}.$$

Wählt man daher für $\mathfrak{k}(z)$ eine Form, welche die verlangte Eigenschaft besitzt und dabei von möglichst niedrigem Grade in z ist, so kann diese überhaupt keinen Faktor G_1 besitzen. Wir erhalten damit das wichtige Resultat, daß, wenn p eine irreguläre Primzahl ist, dieser auch eine solche Form $\mathfrak{k}(z)$ entspricht, die mod. p ein Teiler von $F(z)$ ist.

Wenn demnach

$$F(z) = \mathfrak{k}(z) K(z) \pmod{p}$$

ist, bezeichnen wir weiter die Wurzeln der Gleichung $\mathfrak{k}(z) = 0$ mit $\alpha_1, \dots, \alpha_s$, diejenigen von $K(z) = 0$ mit $\beta_1, \dots, \beta_{n-s}$. Es müssen dann — nach schon früher erwähnten Sätzen über Kongruenzen mit Primmodul — die Größenreihen

$$\mathfrak{g}_1, \mathfrak{g}_2, \dots, \mathfrak{g}_n$$

und

$$\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_{n-s}$$

mod. $\mathfrak{p}$ übereinstimmen, wenn $\mathfrak{p}$ ein Primideal von p bedeutet. Es wird demnach, wenn man auf (1) zurückgeht, auch

$$\sum_{h=0}^{s-2} \mathfrak{k}_h(\beta_1^{s-h-1} + \alpha_i \beta_1^{s-h-2} + \dots + \alpha_i^{s-h-1}) + \mathfrak{k}_{s-1} \equiv 0 \pmod{\mathfrak{p}}$$

sein. Addiert man die für $i = 1, \dots, s$ entstehenden Kongruenzen, so erhält man, wenn man noch nach Einführung der Bezeichnung

$$\sum_{i=1}^{s} \alpha_i^r = S_r$$

die Newton-Girardschen Formeln:

$$\mathfrak{k}_0 S_r + \mathfrak{k}_1 S_{r-1} + \cdots + \mathfrak{k}_r r = 0 \qquad (r = 1, \cdots, s-1)$$

berücksichtigt:

$$s\mathfrak{k}_0 \beta_1^{s-1} + (s-1)\mathfrak{k}_1 \beta_1^{s-2} + (s-2)\mathfrak{k}_2 \beta_1^{s-3} + \cdots \equiv 0 \pmod{\mathfrak{p}},$$

die, mit $\mathfrak{k}(\beta_1) \equiv 0 \pmod{\mathfrak{p}}$ zusammengestellt, unmittelbar zeigt, daß die Discriminante von $\mathfrak{k}(z)$ durch p teilbar ist.

Das Vorstehende gibt uns endlich das Mittel in die Hand, um für einen gegebenen Gattungsbereich durch eine endliche Reihe rationaler Operationen die irregulären Primzahlen wirklich zu bestimmen, falls solche überhaupt existieren. Man hat dazu nur die Reihe der Teiler mod. p von $F(z)$ aufzustellen, und nachzusehn, ob unter diesen ein solcher $\mathfrak{k}(z)$ existiert, für welchen $\frac{\mathfrak{k}(\mathfrak{g})}{\mathfrak{p}}$ eine ganze Größe ist.

Die Zerlegung der ganzen Größen in Primideale.

§ 26. Die soeben hergeleiteten Sätze liefern uns alle Mittel an die Hand, um eine beliebige ganze Größe des Gattungsbereichs, insofern diese von 0 verschieden und auch keine Einheit ist, als Produkt von Primgrößen durch ein wohldefiniertes Verfahren in der Tat darzustellen. Das Verfahren liefert zugleich einen genaueren Einblick in die Struktur dieser arithmetischen Gebilde, indem sie diese Zerlegung gewissermaßen im Bereiche der aus $[\mathsf{A}, x_1, \ldots, x_m]$ entstammenden Formen abbildet.

Da jede ganze Größe ein Teiler ihrer Norm, diese Norm aber einer Form des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ äquivalent ist, und endlich jede solche Form als Produkt ebensolcher Primformen geschrieben werden kann, genügt es, die Zerlegung der Primformen P des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ wirklich auszuführen. Die hierauf bezüglichen Tatsachen sind so einfach, daß wir am besten tun, den definitiven Satz in seiner endgültigen Fassung vorauszuschicken*).

*) Die Stellung des hier ausgesprochenen Satzes in der Literatur — insbesondere zu Kroneckers Darstellung — erfordert ausführlichere Erörterungen und wird in § 29 nachgeholt.

Es sei $F(z) = 0$ die Fundamentalgleichung der Gattung, P irgend eine Primgröße des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$, mit Ausschluß der irregulären Primzahlen*); man zerlege sodann $F(z)$ in irreduzible Faktoren nach dem Äquivalenzmodul P:

$$F(z) \sim F_1(z)^{\alpha_1} F_2(z)^{\alpha_2} \ldots F_r(z)^{\alpha_r} \text{ (aequ. mod. } P),$$

wo $a_1 l_1 + a_2 l_2 + \cdots + a_r l_r = n$ ist, wenn l_i den Grad von $F_i(z)$ in z bedeutet.

Dann wird der größte gemeinschaftliche Teiler von $F_i(\mathfrak{g})$ und P ein Primideal (auch nicht ~ 1) und kann, da $F_i(\mathfrak{g})$ eine homogene Form der u ist, als ideale Größe geradezu $P + F_i(\mathfrak{g})$ geschrieben werden. Die Zerlegung von P in Primideale ist dann durch die Äquivalenz

$$P \sim (P + F_1(\mathfrak{g}))^{\alpha_1} (P + F_2(\mathfrak{g}))^{\alpha_2} \ldots (P + F_r(\mathfrak{g}))^{\alpha_r} \qquad (1)$$

gegeben.

Es ist endlich (siehe § 27) $P + F_i(\mathfrak{g})$ ein Primideal l_i^{ten} Grades, d. h.

$$\text{Nm.}(P + F_i(\mathfrak{g})) \sim P^{l_i}.$$

Um die in diesem Theoreme zusammengefaßten Tatsachen als richtig zu erweisen, bemerke man vor allem, daß die für $F(z)$ erhaltene Zerlegung nach dem Äquivalenzmodul P unmittelbar die Identität**)

$$\bar{Q} F(z) = Q F_1(z)^{\alpha_1} F_2(z)^{\alpha_2} \ldots F_r(z)^{\alpha_r} - PH(z)$$

nach sich zieht, wo Q und $\bar{Q}$ zu P teilerfremde Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ sind und H eine diesem Bereiche

*) Die Zerlegung der irregulären Primzahlen tragen wir in § 28 nach. Wir hätten wohl eine beide Fälle zugleich umfassende Darstellung geben können; jedoch mit Rücksicht auf die geometrischen und funktionentheoretischen Anwendungen — wo der zweite Fall überhaupt nicht auftritt — schien es angezeigt, diese Betrachtungen vorauszuschicken, in welchen einfachere Hilfsmittel genügen.

**) Es sei nebenbei bemerkt, daß $Q = 1$ ist.

entstammende Form ist, die in z den n^{ten} Grad nicht erreicht. Setzt man in dieser Identität $z = \mathfrak{y}$, so wird:

$$Q F_1(\mathfrak{y})^{a_1} F_2(\mathfrak{y})^{a_1} \dots F_r(\mathfrak{y})^{a_r} = P H(\mathfrak{y}). \qquad (2)$$

Man sieht dann zuerst, daß der größte gemeinschaftliche Teiler von $P + F_i(\mathfrak{y})$ und $P + F_j(\mathfrak{y})$, wenn i von j verschieden ist, ~ 1 sein muß. Es wäre dies ein gemeinschaftlicher Teiler von $F_i(\mathfrak{y})$, $F_j(\mathfrak{y})$ und P, und wenn R die Resultante von $F_i(z)$ und $F_j(z)$ nach z bedeutet, auch ein gemeinschaftlicher Teiler von R und P. Nun ist aber P irreduzibel und R nach § 20 nicht durch P teilbar, also $(R, P) \sim 1$ und auch, wie behauptet, $(P + F_i(\mathfrak{y}), P + F_j(\mathfrak{y})) \sim 1$.

Ist ferner

$$\mathfrak{k}(\mathfrak{y}) = \mathfrak{k}_0 \mathfrak{y}^s + \dots + \mathfrak{k}_s,$$

wo die $\mathfrak{k}_0, \dots, \mathfrak{k}_s$ wieder dem Bereiche $[A, x_1, \dots, x_m]$ entstammende Formen bedeuten und $s < l_i$ ist, so kann $\mathfrak{k}(\mathfrak{y})$ nur dann durch $P + F_i(\mathfrak{y})$ teilbar sein, wenn $\mathfrak{k}(\mathfrak{y})$ durch P teilbar ist, also dasselbe für die einzelnen Koeffizienten $\mathfrak{k}_0, \dots, \mathfrak{k}_s$ stattfindet.

Wäre nämlich $\mathfrak{k}(\mathfrak{y})$ durch $P + F_i(\mathfrak{y})$ teilbar, so könnte man in dem durch P teilbaren Produkte $F_1(\mathfrak{y})^{a_1} \dots F_r(\mathfrak{y})^{a_r}$ auch $F_i(\mathfrak{y})$ durch $\mathfrak{k}(\mathfrak{y})$ ersetzen, ohne daß die Teilbarkeit durch P verloren ginge. Dann ergäbe aber dieses Produkt einen Ausdruck $\mathfrak{K}(\mathfrak{y})$, der in $\mathfrak{y}$ den Grad n nicht erreicht und also nur dann durch P teilbar sein kann, wenn dies für den Koeffizienten jeder Potenz von $\mathfrak{y}$ stattfindet. Nun ist dieser Koeffizient für die höchste Potenz von $\mathfrak{y}$ ein Produkt von zu P teilerfremden Größen mit $\mathfrak{k}_0^{a_i}$. Es müßte also $\mathfrak{k}_0$ durch P teilbar sein. Dann wäre aber auch

$$\mathfrak{k}_1 \mathfrak{y}^{s-1} + \dots + \mathfrak{k}_s$$

durch $P + F_i(\mathfrak{y})$ teilbar, also mit Wiederholung des soeben auseinandergesetzten Schlusses wieder $\mathfrak{k}_1$ durch P teilbar und so fort.

Hieraus folgt weiter, daß $P + F_i(\mathfrak{y})$ eine echte irreduzible Größe (eine Primgröße) ist. Es kann

keinesfalls $P + F_i(\mathfrak{g}) \sim 1$ sein; sonst wäre ja das Produkt $F_1(\mathfrak{g})^{a_1} \dots F_r(\mathfrak{g})^{a_r}$ auch nach Weglassung des Faktors $F_i(\mathfrak{g})^{a_i}$ durch P teilbar, während dies doch ein Ausdruck in $\mathfrak{g}$ ist, der den n^{ten} Grad nicht erreicht, und in welchem der Koeffizient der höchsten Potenz von $\mathfrak{g}$ nicht durch P teilbar ist.

Wäre nun weiter $P + F_i(\mathfrak{g})$ ein Produkt mehrerer Primgrößen, z. B.

$$P + F_i(\mathfrak{g}) \sim \mathfrak{p}\mathfrak{q} \cdots,$$

wo $\mathfrak{p}$ und $\mathfrak{q}$ im Sinne der Äquivalenz von Eins verschieden sind, so hätte man, weil ja jede ganze ideale Größe so darstellbar ist:

$$dE\mathfrak{p} = \mathfrak{k}_{n-1}\mathfrak{g}^{n-1} + \mathfrak{k}_{n-2}\mathfrak{g}^{n-2} + \cdots + \mathfrak{k}_0,$$

wo $(d, P) \sim 1$ und $E, \mathfrak{k}_{n-1}, \dots, \mathfrak{k}_0$ dem Bereiche $[\mathsf{A}, x_1, \dots, x_m]$ entstammende Formen sind, von denen die erste, E, primitiv ist. Nennt man nun Q_i den Koeffizient der höchsten Potenz von z in $F_i(z)$, wo also Q_i eine zu P teilerfremde Form des Bereichs $[\mathsf{A}, x_1, \dots, x_m]$ ist, so erhält man durch Anwendung des gewöhnlichen Divisionsverfahrens

$$dQ_i^{\varkappa} E\mathfrak{p} = F_i(\mathfrak{g})\mathfrak{k}'(\mathfrak{g}) + \mathfrak{k}_0'\mathfrak{g}^{l_i-1} + \cdots + \mathfrak{k}'_{l_i-1}.$$

Es ist demnach $\mathfrak{k}_0'\mathfrak{g}^{l_i-1} + \cdots$ durch $\mathfrak{p}$ teilbar. Also muß die Resultante von $F_i(z)$ und $\mathfrak{k}_0' z^{l_i-1} + \cdots$ mod. P verschwinden, und, da $F_i(z)$ aequ. mod. P irreduzibel ist, auch $\mathfrak{k}_0', \mathfrak{k}_1', \dots \equiv 0$ (mod. P) sein. Hieraus folgt:

$$dQ_i^{\varkappa} E\mathfrak{p} \equiv F_i(\mathfrak{g})\mathfrak{k}'(\mathfrak{g}) \pmod{P},$$

d. h. es müßte $\mathfrak{p}$ durch $\mathfrak{p}\mathfrak{q}$ teilbar sein, was wieder nur dann möglich, wenn im Widerspruch zur Annahme $\mathfrak{q} \sim 1$ wird. D. h. aber $P + F_i(\mathfrak{g})$ ist irreduzibel.

Weiter ist $F_i(\mathfrak{g})$ durch das Primideal $P + F_i(\mathfrak{g})$ teilbar; es kann aber $F_i(\mathfrak{g})$ niemals durch $(P + F_i(\mathfrak{g}))^2$ teilbar sein, wenn $a_i > 1$ ist. $F_i(\mathfrak{g})$ ist keinesfalls durch ein in P enthaltenes, von $P + F_i(\mathfrak{g})$ verschiedenes Primideal teilbar, da ja sonst $P + F_i(\mathfrak{g})$ durch diese beiden verschiedenen Primideale teilbar, also kein Primideal wäre; sollte

nun $F_i(\mathfrak{g})$ durch $(P + F_i(\mathfrak{g}))^2$ teilbar sein, so kann P nicht durch $(P + F_i(\mathfrak{g}))^2$ teilbar sein, da dies sonst auch für den größten gemeinschaftlichen Teiler von P und $F_i(\mathfrak{g})$, das ist für das Primideal $P + F_i(\mathfrak{g})$, der Fall sein müßte. Es ist also in diesem Falle

$$F_i(\mathfrak{g}) \sim (P + F_i(\mathfrak{g}))^e \mathfrak{q}_1$$
$$P \sim (P + F_i(\mathfrak{g}))\, \mathfrak{q}_2$$

und $(\mathfrak{q}_1, P) \sim 1$; wo nun nachzuweisen bleibt, daß $e = 1$ sein muß. In diesem Falle ist aber nicht nur

$$F_1(\mathfrak{g})^{a_1} \ldots F_i(\mathfrak{g})^{a_i} \ldots F_r(\mathfrak{g})^{a_r},$$

sondern auch schon, wenn man an die Stelle von a_i die Eins setzt,

$$F_1(\mathfrak{g})^{a_1} \ldots F_i(\mathfrak{g}) \ldots F_r(\mathfrak{g})^{a_r}$$

durch P teilbar. Für die von $P + F_i(\mathfrak{g})$ verschiedenen, in P enthaltenen Primideale ändert sich nichts, da diese ja zu $F_i(\mathfrak{g})$ teilerfremd sind; das Primideal $P + F_i(\mathfrak{g})$ aber, das nur einmal in P enthalten ist, ist schon ein Teiler von $F_i(\mathfrak{g})$. Dann muß endlich $a_i = 1$ sein. Sonst wäre im zweiten Produkte der Grad in Bezug auf $\mathfrak{g}$ kleiner als n, und das Produkt doch durch P teilbar, während die Koeffizienten nicht sämtlich (insbesondere der Koeffizient der höchsten Potenz von $\mathfrak{g}$ nicht) durch P teilbar sind.

Die zu Beginn dieses Paragraphen angegebene Zerlegung von P ist nunmehr eine einfache Folge der soeben auseinandergesetzten Teilsätze.

Die aus der Zerlegung von $F(z)$ nach dem Äquivalenzmodul P hervorgehende Identität zeigt unmittelbar, daß P ein Teiler von

$$F_1(\mathfrak{g})^{a_1} \ldots F_i(\mathfrak{g})^{a_i} \ldots F_r(\mathfrak{g})^{a_r};$$

daraus folgt aber weiter, daß P einem Potenzprodukte der Primideale

$$P + F_1(\mathfrak{g}), \ldots, P + F_i(\mathfrak{g}), \ldots, P + F_r(\mathfrak{g})$$

äquivalent sein muß. Ist $a_i = 1$, so könnte eventuell $F_i(\mathfrak{g})$ durch eine höhere Potenz von $P + F_i(\mathfrak{g})$ teilbar sein, aber

P ist dann nur durch $P + F_i(\mathfrak{y})$, nicht aber durch $(P + F_i(\mathfrak{y}))^2$ teilbar. In diesem Falle ist also der entsprechende Teiler von P in der Tat $(P + F_i(\mathfrak{y}))^{a_i}$.

Ist aber $a_i > 1$, so ist der entsprechende Teiler in P jedenfalls $(P + F_i(\mathfrak{y}))^{b_i}$ und $b_i \leqq a_i$. Wäre aber $b_i < a_i$, so müßte auch schon

$$F_1(\mathfrak{y})^{a_1} \ldots F_i(\mathfrak{y})^{b_i} \ldots F_r(\mathfrak{y})^{a_r}$$

durch P teilbar sein. Das ist aber unmöglich, denn das soeben hingeschriebene Produkt ist ein Ausdruck, der in $\mathfrak{y}$ den n^{ten} Grad nicht erreicht, und in dem der Koeffizient der höchsten Potenz von $\mathfrak{y}$ durch P nicht teilbar ist.

Damit ist aber die unter (1) aufgestellte Zerlegung von P in Primideale als richtig erwiesen.

§ 27. Im Anschlusse an die in der Theorie der algebraischen Zahlen gebräuchliche Ausdrucksweise soll eine Primform des Bereichs $[A, x_1, \ldots, x_m]$, die durch das Quadrat eines Primideals des vorgelegten Gattungsbereichs teilbar ist, als kritische Primform der Gattung bezeichnet werden.

Es zeigt sich dann leicht, daß die in der Discriminante der Fundamentalgleichung enthaltenen Primformen des Bereichs $[A, x_1, \ldots, x_m]$ und nur diese kritische Primformen der Gattung sind*). Der Satz gilt auch für die irregulären Primzahlen, falls solche existieren. Den Beweis tragen wir am Schluß des Paragraphen nach. Ob

*) Für den Fall der algebraischen Zahlen hat R. Dedekind in einer großen Arbeit diesen Satz zuerst bewiesen („Über die Discriminanten endlicher Körper." Abhandl. d. Göttinger Ges. d. Wiss. Bd. XXIX 1882.) Die tiefgehenden, schwierigen Methoden dieser Abhandlung sind wohl kaum zu vermeiden, wenn man, wie es darin geschieht, prinzipiell die Einführung unbestimmter Größen vermeiden will.

Mit Hilfe der Kroneckerschen Methoden hat K. Hensel in der früher citierten Abhandlung den Satz für die Theorie der algebraischen Zahlen zuerst vollständig bewiesen; bei Kronecker bleibt die Stellung der in $(n - 2)!$ enthaltenen natürlichen Primzahlen noch fraglich.

P eine kritische Primform ist, zeigt sich ja unmittelbar bei der Zerlegung von $F(z)$ nach dem Äquivalenzmodul P. Es ist dies dann und nur dann der Fall, wenn bei dieser Zerlegung mehrfache Faktoren auftreten, oder also die Discriminante der Fundamentalgleichung durch P teilbar ist. Ist P eine natürliche Primzahl, so ist diese letzte Formulierung der gesuchten Bedingung unmittelbar klar; aber sie ist auch dann leicht einzusehn, wenn P Unbestimmte, z. B. x, enthält. Die Zerlegung ergibt sich dann aus der Zerlegung von $[F(z)]_\xi$, wenn ξ eine Wurzel der Gleichung $P(x_1) = 0$ bedeutet. Und mehrfache Faktoren sind dann und nur dann vorhanden, wenn $[\text{Dscr. } F(z)]_\xi = 0$, oder also Dscr. $F(z)$ durch P teilbar ist.

Der Fall, wo P nur durch die erste Potenz von $P + F_i(\mathfrak{z})$ teilbar ist, wird demnach als der allgemeine zu betrachten sein; für diesen gilt die folgende wichtige Bemerkung. Gerade dann, wenn $a_i = 1$, könnte $F_i(\mathfrak{z})$ auch noch durch $(P + F_i(\mathfrak{z}))^2$ teilbar sein; nun ist aber die Form $F_i(z)$, die bei der Zerlegung von $F(z)$ auftritt, unbeschadet der Gültigkeit aller Resultate mit irgend einer Form $\overline{F}_i(z)$, die $\equiv F_i(z) \pmod{P}$, vertauschbar. Ist also $F_i(\mathfrak{z})$ in der Tat durch $(P + F_i(\mathfrak{z}))^2$ teilbar, so hat man nur statt $F_i(z)$ jetzt $F_i(z) + Pu_1^n$ einzuführen, und erhält damit eine Form, die nur mehr durch $P + F_i(\mathfrak{z})$ und nicht durch $(P + F_i(\mathfrak{z})^2$ teilbar ist.

In den folgenden Betrachtungen denken wir uns diese Änderung an $F_i(z)$, sofern dies notwendig erscheint, schon als ausgeführt, also $F_i(\mathfrak{z})$ als durch $(P + F_i(\mathfrak{z}))^2$ nicht teilbar gewählt.

Wir gehn nun auf die Identität

$$\overline{Q}\, F(z) = Q F_1(z)^{a_1} \ldots F_i(z)^{a_i} \ldots - PH(z)$$

zurück. Es seien ferner

$$\xi_1, \xi_2, \ldots, \xi_{l_i}$$

die Wurzeln der Gleichung $F_i(z) = 0$. Setzt man diese Werte für z in die eben hingeschriebene Identität, so erhält man

$$\overline{Q}^{l_i} \prod_{j=1}^{l_i} F(\xi_j) = (-1)^{l_i} P^{l_i} \prod_{j=1}^{l_i} H(\xi_j).$$

Nun ist (Kap. III. § 24) für die Resultante von $F(z)$ und $F_i(z)$ nach z, wenn Q_i wieder den Koeffizienten der höchsten Potenz von z in $F_i(z)$ bedeutet:

$$\text{Res.}\,(F(z),\, F_i(z)) = (-1)^{n l_i} Q_i^n \prod_{j=1}^{l_i} F(\xi_j)$$

$$= \prod_{j=1}^{n} F_i(z_j),$$

wenn $z_1, \ldots, z_n$ die Wurzeln der Gleichung $F(z) = 0$ bezeichnen, also weiter auch

$$= \text{Nm.}\, F_i(\mathfrak{g}),$$

und endlich Nm. $F_i(\mathfrak{g})$ durch P^{l_i} teilbar. Da ferner $F_i(\mathfrak{g})$ nur das eine Primideal $P + F_i(\mathfrak{g})$ von P enthält und auch für dieses nur durch $P + F_i(\mathfrak{g})$, nicht aber durch $(P + F_i(\mathfrak{g}))^2$ teilbar ist, erhält man endlich Nm. $F_i(\mathfrak{g}) \sim \text{Nm}\,(P + F_i(\mathfrak{g}))\, Q$, wo $(P, Q) \sim 1$, und daher

$$\text{Nm.}\,(P + F_i(\mathfrak{g})) \sim P^{l_i + e_i},$$

wo noch nachzuweisen bleibt, daß $e_i = 0$ ist.

Dies ergibt sich aber aus der Identität (2) des § 26:

$$Q F_1(\mathfrak{g})^{a_1} F_2(\mathfrak{g})^{a_2} \ldots F_r(\mathfrak{g})^{a_r} = P H(\mathfrak{g}).$$

In dieser kann $H(\mathfrak{g})$ durch kein Primideal von P teilbar sein; denn das Produkt links und P enthalten die Primideale von P in gleicher Potenz. Für $a_i > 1$ wurde dies schon früher nachgewiesen; für $a_i = 1$ haben wir eben unter den kongruenten Formen F_i eine entsprechende gewählt. Demnach ist $(\text{Nm.}\, H(\mathfrak{g}),\, P) \sim 1$. Wäre nun auch nur ein e_i eine von 0 verschiedene, nicht negative ganze Zahl, so wäre die Norm des Ausdrucks links durch eine höhere als die n^{te} Potenz von P teilbar. Das ist aber nicht möglich, denn dieselbe Norm ergibt sich unmittelbar durch den Ausdruck P^n Nm. $H(\mathfrak{g})$.

Es ist demnach, wie noch nachzuweisen war, $P + F_i(\mathfrak{g})$ ein Primideal l_i^{ten} Grades, d. h. Nm. $(F + F_i(\mathfrak{g})) \sim P^{l_i}$, wenn l_i den Grad von $F_i(z)$ in z bedeutet.

Es ist endlich noch zu zeigen, daß — falls solche überhaupt existieren — auch die irregulären Primzahlen kritische Primzahlen sind.

In diesem Falle gibt es eine Form niedrigsten, s^{ten} Grades ($s \leq n-1$), von der Beschaffenheit, daß $\mathfrak{k}(\mathfrak{z})$ durch p teilbar ist. Diese Form enthält, wie wir am Schlusse vom § 25 gezeigt haben, mod. p ein $F_i(z)$ mindestens zum Quadrat als Teiler. Es ist auch jetzt Nm. $F_i(\mathfrak{z})$ durch p^{l_i} teilbar; denn die hierauf bezüglichen, soeben gegebenen Entwicklungen sind von allen weiteren, sonst benutzten Voraussetzungen frei. Mithin ist $F_i(\mathfrak{z})$ durch gewisse in p enthaltene Primideale, $\mathfrak{p}, \mathfrak{q}, \ldots$ teilbar. Dann muß aber p auch durch $\mathfrak{p}^2, \mathfrak{q}^2, \ldots$ teilbar sein; sonst hätte schon die durch

$$F_i(z)\,\bar{\mathfrak{k}}(z) \equiv \mathfrak{k}(z) \pmod{p}$$

bestimmte Form vom Grade $s - l_i$ die für $\mathfrak{k}(z)$, als Form niedrigsten Grades supponierte Eigenschaft*).

§ 28. Die Zerlegung der irregulären Primzahlen eines Gattungsbereichs — falls solche vorhanden sind — erfolgt nach denselben Prinzipien, wenn auch das Schlußresultat nicht jene elegante Einfachheit zeigt, die das Zerlegungsgesetz der regulären Primzahlen und Primformen auszeichnet.

Auch in diesem Falle folgt aus

$$F_1(\mathfrak{z})^{a_1} \ldots F_r(\mathfrak{z})^{a_r} \equiv 0 \pmod{p},$$

daß jedes

$$p + F_1(\mathfrak{z}), \cdots, p + F_r(\mathfrak{z})$$

ein Teiler von p und nicht ~ 1 ist, weil der Nachweis, daß

---

*) In der Theorie der algebraischen Zahlen bedeutet Nm. $\mathfrak{p}$ auch die Anzahl der mod. $\mathfrak{p}$ inkongruenten Zahlen. Darauf fußend, beweist man, daß Nm. $(p + F_i(\mathfrak{z})) \sim p^{l_i}$, ohne Rücksicht darauf, ob p regulär ist oder nicht. Daraus folgt dann leicht, daß in diesem Falle überhaupt keine irregulären Primzahlen existieren. (S. diesbezüglich die früher citierte Abhandlung von K. Hensel, sowie die ausführliche Darstellung in H. Webers „Lehrbuch der Algebra".)

Nm. $(p + F_i(\mathfrak{g})) \sim p^{h_i}$ ist, von den für p geltenden engeren Voraussetzungen unabhängig bleibt. Ebenso ist wieder

$$(p + F_i(\mathfrak{g}),\ p + F_j(\mathfrak{g})) \sim 1,$$

weil $F_i(z)$ und $F_j(z)$ (mod. p) irreduzible und nicht äquivalente Formen sind. Endlich muß jedes in p enthaltene Primideal Teiler einer der Größen $p + F_1(\mathfrak{g}), \cdots$ sein. Es kommt also nur darauf an, nachzuweisen, daß diese Größen Primideale sind. Dann muß für p die Zerlegung

$$p \sim (p + F_1(\mathfrak{g}))^{b_1} \cdots (p + F_r(\mathfrak{g}))^{b_r}$$

stattfinden, wo $b_1 \leqq a_1, \ldots$. Allerdings fehlt dann noch die genauere Bestimmung der Exponenten $b_1, \ldots, b_r$, die aber durch eine endliche Versuchsreihe erfolgen kann. Man hat hierzu nur zu prüfen, welche der Größen

$$\frac{p}{p + F_1(\mathfrak{g})},\quad \frac{p}{(p + F_1(\mathfrak{g}))^2}, \cdots$$

ganz sind.

Wir erledigen also das vorliegende Problem vollständig durch den Nachweis, daß $p + F_i(\mathfrak{g})$ ein Primideal ist. (Die angewandte Methode beruht teilweise auf einem von K. Hensel herrührenden Gedanken.)

Angenommen, dies sei nicht der Fall, und

$$\mathfrak{p} + F_i(\mathfrak{g}) \sim \mathfrak{p}\mathfrak{q},$$

wo $\mathfrak{q}$ im Sinne der Äquivalenz von Eins verschieden, so kann man nach früher bewiesenen Sätzen eine wirkliche Größe des Gattungsbereichs

$$\alpha \sim \mathfrak{p}\mathfrak{a}$$

so bestimmen, daß $(\mathfrak{a}, \mathfrak{q}) \sim 1$ ist. Diese Größe α sei durch das Fundamentalsystem folgendermaßen ausgedrückt:

$$\alpha = a_1\mu_1 + \cdots + a_r\mu_r.$$

Die Fundamentalgröße $\mathfrak{g}$ geht, wenn man an die Stelle von $u_1, \ldots, u_r$ jetzt $a_1, \ldots, a_r$ setzt, demnach in α über.

Die Tatsache, daß $F_i(\mathfrak{g})$ durch $\mathfrak{p}\mathfrak{q}$ teilbar ist, bleibt auch dann richtig, wenn man für die Unbestimmten $u_1, \ldots, u_r$ irgend

welche ganze Größen setzt. Schreibt man demnach $F_i(\mathfrak{z})$ ausführlicher $F_i(\mathfrak{z}, u_1, \ldots, u_r)$, und setzt jetzt $u_1 + a_1, \ldots, u_r + a_r$ an Stelle von $u_1, \ldots, u_r$, so wird auch

$$F_i(\mathfrak{z} + \alpha, u_1 + a_1, \ldots, u_r + a_r) \equiv 0 \pmod{\mathfrak{p}\mathfrak{q}}. \quad (1)$$

Da aber $\alpha \equiv 0 \pmod{\mathfrak{p}}$, haben demnach die Kongruenzen

$$F_i(z, u_1, \ldots, u_r) \equiv 0 \pmod{\mathfrak{p}}$$
$$F_i(z, u_1 + a_1, \ldots, u_r + a_r) \equiv 0 \pmod{\mathfrak{p}}$$

eine gemeinschaftliche Wurzel. Ihre Resultante muß mod. $\mathfrak{p}$ und demnach auch mod. p verschwinden. Da aber $F_i(z) \pmod{p}$ irreduzibel ist, ferner die beiden Formen von gleichem Grade sind, und endlich auch in der zweiten Form der Koeffizient von z^{l_i} gleich Eins ist, erhellt hieraus, daß

$$F_i(z, u_1 + a_1, \ldots, u_r + a_r) \equiv F_i(z, u_1, \ldots, u_r) \pmod{p}. \quad (2)$$

Demnach ist endlich mit Benutzung von (1):

$$F_i(\mathfrak{z} + \alpha, u_1, \ldots, u_r) \equiv 0 \pmod{\mathfrak{p}\mathfrak{q}} \quad (3)$$

eine Teilbarkeitsbestimmung, die erhalten bleiben muß, wenn man für die u beliebige ganze Größen setzt, also z. B. $u_1 = 0, \ldots, u_r = 0$ wählt. Dann wäre aber

$$\alpha^{l_i} \equiv 0 \pmod{\mathfrak{p}\mathfrak{q}},$$

und das ist der Annahme nach gewiß unmöglich, wenn $\mathfrak{q}$ ein im Sinne der Äquivalenz von $\mathfrak{p}$ verschiedenes Primideal enthält.

Es bleibt also nur noch der Fall zu untersuchen, wo $\mathfrak{q}$ eine Potenz des Primideals $\mathfrak{p}$ ist. Dann ist aber α der Annahme nach nur durch $\mathfrak{p}$ und nicht durch $\mathfrak{p}^2$ teilbar, und es ist jedenfalls aus (3):

$$F_i(\mathfrak{z} + \alpha, u_1, \ldots, u_r) \equiv 0 \pmod{\mathfrak{p}^2}.$$

Entwickelt man den Ausdruck links nach Potenzen von α, so wird

$$F_i(\mathfrak{z}) + F_i'(\mathfrak{z})\,\alpha + \tfrac{1}{2} F_i''(\mathfrak{z})\,\alpha^2 + \cdots \equiv 0 \pmod{\mathfrak{p}^2}.$$

Hier ist aber $F_i(\mathfrak{z})$, α^2, α^3, ... durch $\mathfrak{p}^2$ teilbar. Dasselbe müßte also für $F_i'(\mathfrak{z})\,\alpha$ stattfinden, und es wäre endlich

$$F_i'(\mathfrak{z}) = 0 \pmod{\mathfrak{p}}.$$

Da aber auch $F_i(\mathfrak{z}) \equiv 0 \bmod \mathfrak{p}$ ist, müßte die Resultante von $F_i(z)$ und $F_i'(z)$ mod. $\mathfrak{p}$ verschwinden, und dies ist wegen der Irreduzibilität von $F_i(z)$ unmöglich. Damit ist aber der fragliche Satz in allen Teilen bewiesen.

§ 29. Die mit diesem Satze gewonnene Erkenntnis — eine beinahe unerschöpfliche Quelle neuer Untersuchungen — verdanken wir der bewundernswerten Intuition Kroneckers. Diese Intuition ist um so merkwürdiger, als die von Kronecker gegebenen Sätze einer Richtigstellung in ihrem wesentlichsten Punkte bedürfen. Nur in der Theorie der algebraischen Zahlen und der algebraischen Funktionen einer Veränderlichen, wenn von den Zahlenkoeffizienten abgesehn wird, sind die Kroneckerschen Resultate unbedingt richtig; im allgemeinen Falle aber nur, wenn es sich um die Zerlegung einer natürlichen Primzahl handelt. Enthält P Unbestimmte, so ergibt das von Kronecker angegebene Verfahren zur Zerlegung von P im allgemeinen geradezu falsche Resultate.

Dieses merkwürdige Versehn Kroneckers beruht, wie es scheint, darauf, daß er die bei der Zerlegung einer Form mod. P auftretenden irreduziblen Formen als Primformen für den Modul P ansieht, dies aber — wie in § 19 auseinandergesetzt wurde — im allgemeinen nicht der Fall ist.

Genauer formuliert verlangt Kronecker die Zerlegung von $F(z)$ nicht aequ. mod. P, sondern nur mod. P; daß es sich dabei um ein wirkliches Versehn handelt, ist aus den Einzelnheiten der Deduktion klar zu ersehen, um so mehr, als die komplizierte Begriffsbildung des Äquivalenzmoduls der Festschrift völlig fremd bleibt.

Da es sich um das eigentliche Fundament der arithmetischen Theorie der algebraischen Größen — also um einen Gegenstand höchster Wichtigkeit — handelt, soll der Tatbestand an einem einfachen Beispiele noch ausführlich auseinandergesetzt werden.

Die Gleichung

$$z^2 = x^2 - 4t,$$

wo x und t Unbestimmte sind, definiert einen Gattungsbereich

$(\sqrt{x^2-4t})$, der dem Bereiche $([1], x, t)$ entstammt. Die Discriminante der Gleichung ist $4(x^2-4t)$ und die wirklichen absolut ganzen Größen in $(\sqrt{x^2-4t})$ haben also jedenfalls die Gestalt:

$$\frac{X_1 + X_2\sqrt{x^2-4t}}{4(x^2-4t)},$$

wo X_1 und X_2 dem angegebenen Formenbereiche angehören. Die Bestimmung eines Fundamentalsystems ist hier von beinahe trivialer Einfachheit, so daß es sich nicht lohnt, die allgemeinen Methoden buchstäblich anzuwenden. Soll $X_1 + X_2\sqrt{x^2-4t}$ durch $4(x^2-4t)$ teilbar sein, so muß dies auch für $X_1 - X_2\sqrt{x^2-4t}$, also weiter für $2X_1$ der Fall sein, es muß also endlich X_1 durch $2(x^2-4t)$ teilbar sein. Weiter muß auch $2X_2\sqrt{x^2-4t}$ durch $4(x^2-4t)$, also $4X_2^2(x^2-4t)$ durch $16(x^2-4t)^2$, und X_2^2 durch $4(x^2-4t)$, oder endlich X_2 durch $2(x^2-4t)$ teilbar sein. Die absolut ganzen Größen in $(\sqrt{x^2-4t})$ besitzen also jedenfalls die Gestalt

$$\frac{X_1 + X_2\sqrt{x^2-4t}}{2};$$

und diese Größen sind umgekehrt in der Tat absolut ganz, wenn $X_1^2 - X_2^2(x^2-4t)$ durch 4 teilbar ist, also wenn die Kongruenz

$$X_1^2 - X_2^2 x^2 \equiv 0 \pmod 4$$

besteht. Dann muß aber wenigstens eine der Kongruenzen

$$X_1 + X_2 x \equiv 0 \quad \text{oder} \quad X_1 - X_2 x \equiv 0 \pmod 2$$

bestehen. Da aber endlich irgend eine dieser Kongruenzen eine Folge der andern ist, also z. B. $X_1 = X_2 x + 2X_3$ geschrieben werden kann, erhält man weiter für die absolut ganzen Größen in $(\sqrt{x^2-4t})$ die notwendige Gestalt:

$$X_3 + X_2\frac{x+\sqrt{x^2-4t}}{2}$$

und endlich, da $\frac{x+\sqrt{x^2-4t}}{2}$ in der Tat eine absolut ganze

Größe des Gattungsbereichs ist, für diesen das Fundamentalsystem:

$$1, \frac{x+\sqrt{x^2-4t}}{2}.$$

Die Fundamentalgröße des Gattungsbereichs ist demnach

$$u_1 + \frac{x+\sqrt{x^2-4t}}{2} u_2;$$

und die Fundamentalgleichung:

$$\left(z - u_1 - \frac{x+\sqrt{x^2-4t}}{2} u_2\right)\left(z - u_1 - \frac{x-\sqrt{x^2-4t}}{2} u_2\right) = 0$$

oder ausgerechnet

$$z^2 - z(2u_1 + u_2 x) + u_1^2 + u_1 u_2 x + u_2^2 t = 0.$$

Wollte man nun nach der Kroneckerschen Anweisung $P = x^2 - 4t$ in Primideale zerlegen, so wäre — nach den in der Fußnote zu § 19 ausgeführten Rechnungen, wo nur z, u_1, u_2 für z_1, z_2, z_3 zu setzen ist — die linke Seite der Fundamentalgleichung mod. $(x^2 - 4t)$ irreduzibel, also $x^2 - 4t$ ein Primideal, was offenbar falsch, da $x^2 - 4t = (\sqrt{x^2-4t})^2$, und Nm. $\sqrt{x^2-4t} \sim x^2 - 4t$ und nicht ~ 1 ist.

Zerlegt man aber der hier gegebenen Anweisung entsprechend nach dem Äquivalenzmodul P, so erhält man

$$P \sim \left(2u_1 + (x + \sqrt{x^2-4t})\, u_2 - 2u_1 - x u_2\right)^2$$

oder also

$$P \sim (\sqrt{x^2-4t})^2,$$

das richtige Resultat.

Die Discriminante der Gattung.

§ 30. Die Discriminante der Fundamentalgleichung kann immer in der Gestalt

$$\mathfrak{D} = D\mathfrak{E}$$

geschrieben werden, wo $\mathfrak{E}$ eine dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammende primitive Form, D eine Form aus $[\mathsf{A}, x_1, \ldots, x_m]$ und zwar ein Potenzprodukt der kritischen Primformen ist.

Die Discriminante der Fundamentalgleichung bestimmt einen gewissen Komplex von Eigenschaften, die der Gattung als solcher eigentümlich sind, d. h. ganz unabhängig davon bleiben, wie die Gattung ursprünglich definiert wurde; dementsprechend ist sie im Sinne einer gewissen Äquivalenz eindeutig bestimmt und — nach einem von Kronecker gebrauchten Ausdruck — eine „Invariante der Gattung" im höheren Sinne des Wortes. Genau ausgedrückt bedeutet dies, daß, wenn man von verschiedenen Definitionen der Gattung ausgehend und bei Benutzung beliebiger Fundamentalsysteme als Discriminante der Gattung das eine Mal D', das andere Mal D'' erhält, D' und D'' im Formenbereiche $[\mathsf{A}, x_1, \ldots, x_m]$ äquivalent sind, wenn A einen orthoiden Bereich bedeutet. Ist aber $A = [1]$, so ist dies erst dann der Fall, wenn wir die in D' und D'' enthaltenen irregulären Primzahlen als Faktoren weglassen.

Um dies zu beweisen, nehmen wir an, man sei bei zwei verschiedenen Definitionen derselben Gattung zu den zwei verschiedenen Fundamentalsystemen

$$\lambda_1, \lambda_2, \ldots, \lambda_s \quad \text{und} \quad \mu_1, \mu_2, \ldots, \mu_r$$

gelangt, denen also die Fundamentalgrößen

$$\mathfrak{f} = \sum_{i=1}^{s} \lambda_i u_i, \quad \mathfrak{g} = \sum_{j=1}^{r} \mu_j v_j$$

entsprechen. Die konjugierten Werte dieser Fundamentalgrößen seien $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ resp. $\mathfrak{g}_1, \ldots, \mathfrak{g}_n$.

Da $\mathfrak{f}$ und $\mathfrak{g}$ ideale ganze Größen derselben Gattung und auch Fundamentalgrößen sind, erhält man unmittelbar die Identitäten

$$d\,\mathfrak{f}_i^k = \mathfrak{a}_{k0} + \mathfrak{a}_{k1}\,\mathfrak{g}_i + \cdots + \mathfrak{a}_{k,n-1}\,\mathfrak{g}_i^{n-1},$$
$$d\,\mathfrak{g}_i^k = \mathfrak{b}_{k0} + \mathfrak{b}_{k1}\,\mathfrak{f}_i + \cdots + \mathfrak{b}_{k,n-1}\,\mathfrak{f}_i^{n-1},$$
$$(i = 1, \ldots, n;\ k = 0, \ldots, n-1),$$

wo die $\mathfrak{a}$ und $\mathfrak{b}$ rationale und ganze ideale Größen des Bereichs sind, also weiter:

$$d^N |\mathfrak{f}_i^k|^2 = \mathfrak{A} |\mathfrak{g}_i^k|^2,$$
$$d^N |\mathfrak{g}_i^k|^2 = \mathfrak{B} |\mathfrak{f}_i^k|^2$$

und

$$\mathfrak{A}\mathfrak{B} = d^{2N}.$$

Demnach sind die rationalen und ganzen idealen Größen $\mathfrak{A}$ and $\mathfrak{B}$ nach Weglassung der in ihnen enthaltenen irregulären Primzahlen Einheiten; d. h. sie sind dann Quotienten von dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ entstammenden primitiven Formen. Weiter aber sind jene Determinantenquadrate $|\mathfrak{f}_i^k|^2$ und $|\mathfrak{g}_i^k|^2$ nichts anderes als die Discriminanten $\mathfrak{D}'$ und $\mathfrak{D}''$ der Fundamentalgleichungen der Gattung, wie sie sich bei den zwei verschiedenen Definitionen ergeben. Es ist also der größte gemeinschaftliche Teiler der in $\mathfrak{D}$ oder $\mathfrak{D}'$ als Koeffizienten auftretenden, dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehörenden Formen nach Weglassung der irregulären Primzahlen derselbe, wie zu beweisen war.

Diese Entwicklungen führen endlich zu dem wichtigen Begriffe der Gattungsdiscriminante, deren Einführung insbesondere für die algebraischen Anwendungen der Theorie von prinzipieller Wichtigkeit ist.

Sind $\alpha_1, \alpha_2, \ldots, \alpha_n$ irgend welche — wirkliche — ganze Größen des Gattungsbereichs und $\alpha_{i1}, \ldots, \alpha_{in}$ die konjugierten Werte von α_i, so nennt man $|\alpha_{ij}|^2$ die Discriminante der Größen $\alpha_1, \ldots, \alpha_n$. Ist nun $\mu_1, \ldots, \mu_r$ $(r \geqq n)$ ein Fundamentalsystem der wirklichen ganzen Größen der Gattung, so kann man aus ihnen auf $\binom{r}{n}$ verschiedene Weisen n Größen

$$\mu_{s_1}, \mu_{s_2}, \ldots, \mu_{s_n}$$

wählen und deren Discriminante Δ_s bilden.

Die $\binom{r}{n}$ Discriminanten $\Delta_1, \Delta_2, \ldots$ bilden dann — nach Kronecker — ein fundamentales Discriminantensystem der Gattung. Und die Discriminante der Gattung ist endlich nichts anderes als der größte gemeinschaftliche Teiler der in dem fundamentalen Discriminantensysteme enthaltenen, dem Bereiche $[\mathsf{A}, x_1, \ldots, x_m]$ angehörigen Größen.

Man hat unmittelbar, wenn $\mathfrak{f}$ die Fundamentalgröße bezeichnet:

$$d\,\mu_{s_j i} = \mathfrak{c}_{j0} + \mathfrak{c}_{j1}\,\mathfrak{f}_i + \cdots + \mathfrak{c}_{j,n-1}\,\mathfrak{f}_i^{n-1}$$

und

$$d^a\,|\,\mu_{s_j i}\,| = \mathfrak{C}\,|\,\mathfrak{f}_i^k\,|\,;$$

es ist also jedes $d^a\,|\,\mu_{s_j i}\,|$ durch $|\,\mathfrak{f}_i^k\,|$ teilbar, wo die Teilbarkeit im Bereiche der idealen ganzen Größen zu verstehen ist.

Es ergibt sich aber auch, wie wir schon früher (§ 24) gesehen haben:

$$\mathfrak{f}_i^k = \mathfrak{h}_{k1}\,\mu_1 + \cdots + \mathfrak{h}_{kr}\,\mu_r$$
$$(k = 0, 1, \ldots, n-1),$$

also

$$|\,\mathfrak{f}_i^k\,| = \sum_{s=1}^{\binom{n}{r}} \mathfrak{H}_s\,|\,\mu_{s_j i}\,|\,.$$

Es entsteht also $|\,\mathfrak{f}_i^k\,|^2$, die Discriminante der Fundamentalgleichung, aus dem größten gemeinschaftlichen Teiler der Discriminanten $|\,\mu_{s_j i}\,|^2$ durch Multiplikation mit einem gewissen Potenzprodukte der irregulären Primzahlen. Dabei ist die Teilbarkeit im Bereiche der idealen ganzen Größen zu verstehen.

§ 31. Wie unmittelbar zu sehen, ist auch das Produkt irgend zweier Determinanten $|\,\mu_{s_j i}\,|$ eine Form aus $[A, x_1, \ldots, x_m]$, und der größte gemeinschaftliche Teiler dieser Produkte wieder die Discriminante der Gattung. Demzufolge kann man endlich eine der Discriminante der Gattung äquivalente Größe, die s. g. Discriminantenform der Gattung — nach der von Kronecker eingeführten Benennung — unmittelbar hinschreiben. Es ist dies das Determinantenquadrat:

$$|\,\mu_{ij}\,|^2 \quad (i, j = 1, \ldots, r),$$

wo $r \geqq n$ ist und $\mu_{i1}, \ldots, \mu_{in}$ die n konjugierten Werte des im Fundamentalsysteme enthaltenen Elementes μ_i bedeuten, während die μ_{ij}, wenn $j > n$, durchweg verschiedene neue Unbestimmte sein sollen. Man sieht dann unmittelbar, daß die Discriminantenform der Gattung eine dem Bereiche

$[\mathsf{A}, x_1, \ldots, x_m]$ entstammende Form ist, in welcher der größte gemeinschaftliche Teiler der Koeffizienten geradezu die Discriminante der Gattung ergibt.

Die Discriminantenform der Gattung, oder noch genauer ausgedrückt, das fundamentale Discriminantensystem ist abermals eine Invariante der Gattung, die einen Komplex von Eigenschaften, die der Gattung als solcher eigentümlich sind, ausdrückt. Ist nämlich $D_1, D_2, \ldots$ ein fundamentales Discriminantensystem, so ist das Divisorensystem

$$(D_1, D_2, \ldots)$$

eine absolute Invariante der Gattung, so daß, wenn bei zwei verschiedenen Definitionen der Gattung und bei Benutzung zweier verschiedener Fundamentalsysteme $\lambda_1, \ldots, \lambda_s$ und $\mu_1, \ldots, \mu_r$ die beiden fundamentalen Discriminantensysteme $D_1', D_2', \ldots$ und $D_1, D_2, \ldots$ entstehen, die beiden ihnen entsprechenden Divisorensysteme eigentlich äquivalent sind:

$$(D_1', D_2', \ldots) \simeq (D_1, D_2, \ldots).$$

Gibt es insbesondere ein Fundamentalsystem von genau n Elementen und ist D dessen Discriminante, so ist auch

$$D \simeq (D_1, D_2, \ldots).$$

Man erkennt die Richtigkeit aller dieser Tatsachen unmittelbar aus der Bemerkung, daß, wenn sowohl $\lambda_1, \ldots, \lambda_s$ als $\mu_1, \ldots, \mu_r$ Fundamentalsysteme sind, hieraus immer Identitäten der Gestalt

$$\lambda_{ij} = a_{1i}\,\mu_{1j} + \cdots + a_{ir}\,\mu_{rj}$$

folgen, wo die a_{ij} Formen des Bereichs $[\mathsf{A}, x_1, \ldots, x_m]$ sind. Hieraus ergibt sich unmittelbar, daß die Determinanten $|\lambda_{ij}|$ homogene und lineare Formen der Determinanten $|\mu_{ij}|$ mit Koeffizienten aus $[\mathsf{A}, x_1, \ldots, x_m]$ sind. Genau ebenso stellt sich also das Produkt aus irgend zwei Determinanten $|\lambda_{ij}|$ als homogene und lineare Form der aus je zwei Determinanten $|\mu_{ij}|$ gebildeten Produkte dar. Das Divisorensystem $(D_1', D_2', \ldots)$ enthält also das Divisorensystem $(D_1, D_2, \ldots)$; genau ebenso ist aber auch $(D_1', D_2', \ldots)$ in $(D_1, D_2, \ldots)$ enthalten; die beiden Divisorensysteme sind mithin in der Tat eigentlich äquivalent (im engeren Sinne des Wortes).

So ergibt denn die Discriminantenform, oder auch das aus ihren Koeffizienten bestehende Divisorensystem die wesentlichen Eigenschaften der Gattung und auch der darin enthaltenen algebraischen Größen in rationaler und ganzer Gestalt. Diese Eigenschaften sind — wenn man den in der Geometrie üblichen Ausdruck in naturgemäß verallgemeinerter Bedeutung anwendet — die Singularitäten der Gattung.

Von diesem Standpunkte aus ist es noch wichtig zu bemerken, daß die Discriminante jeder Fundamentalgleichung und die Gattungsdiscriminante sich genau aus denselben Primformen zusammensetzt. Auch ihre Multiplizität ist im allgemeinen dieselbe, nur die irregulären Primzahlen finden sich, falls solche existieren, in der Discriminante der Fundamentalgleichung mit höherem Exponenten. Es geht dies aus dem Umstande hervor, daß, wenn man den größten gemeinschaftlichen Teiler der Größen

$$\mu_{1i} - \mu_{1j}, \cdots, \mu_{ri} - \mu_{rj}$$

bildet, die Discriminante der Fundamentalgleichung geradezu das Produkt der Quadrate dieser Teiler wird. Jeder solche größte gemeinschaftliche Teiler ist aber, wie unmittelbar zu sehen, auch ein Teiler der Gattungsdiscriminante.

Damit sind die Grundlagen für die Untersuchung jedes speziellen algebraischen Gebildes gegeben. Nur die einfachsten Fälle sind bisher ausführlich bearbeitet. Als solche sind die Theorie der algebraischen Zahlen einerseits, und die Theorie der algebraischen Funktionen einer Veränderlichen, d. h. die Geometrie der ebenen algebraischen Kurven andrerseits zu betrachten.

Sowohl in algebraischer (geometrischer), wie auch in rein arithmetischer Beziehung ist der Ausblick, den die Theorie der algebraischen Größen gewährt, ein unermeßlicher. Und es ist gewiß nicht das geringste Verdienst dieser an Einfachheit und Allgemeinheit kaum übertroffenen Begriffsbildung, daß sie den Gegensatz zwischen Arithmetik und Geometrie in einer höheren Einheit aufhebt.

Namen- und Sachregister.

Die römischen Ziffern bezeichnen die Kapitel, die arabischen Ziffern die Paragraphen.

Abbildung.
Fundamentalsatz für die Theorie der A. V. 10.
Abhängige.
Voneinander a. Formen V. 14.
Absolut.
A. algebraische Größe IV. 7, IX. 1; a. algebraische Größe mod. ($P^{(k)}$) VIII. 9; a. äquivalent I. 5, IX. 13; a. ganze Form IX. 4; a. ganze Größe IX. 4; a. irreduzible Form IV. 18; a. irreduzible Mannigfaltigkeit V. 7; a. irreduzibles Gebilde V. 7.
Absolute.
A. Äquivalenz I. 5, IX. 13; a. Einheit I. 3, IV. 6; a. Invariante der Gattung IX. 31.
Absoluter Rationalitätsbereich IV. 20.
Absolutes.
A. Primsystem VII. 4; a. Primsystem in $[[1], x_1, x_2, \ldots, x_k]$ VIII. 1, 2, 3, 4, 8.
Addition I. 1.
Additionsgesetz, gewöhnliches I. 2.
Adjungierte Größe IV. 5.
Adjunktion I. 4, IV. 5, 7, 21, VIII. 9.
Äquivalent. I, 5.
absolut ä. I. 5, IX. 13; relativ ä. I. 5, 12, IX. 13.
Äquivalente.
Ä. Modul- oder Divisorensysteme VII. 2; mod. ($P^{(k)}$) ä. Divisorensysteme VIII. 5; nach einem Äquivalenzmodul ä. Größen IX. 17.
Äquivalenz I. 5.
Ä. mod. (S) VIII. 1; Ä. rationaler und ganzer Formen IV. 1; Ä. rationaler und ganzer Zahlen IV. 1; absolute Ä. I. 5, IX. 13; engere Ä. VII. 2; engere Ä. mod. ($P^{(k)}$) VIII. 5; Kummersche Ä. IX. 13; relative Ä. I. 5, 12, IX. 13; weitere Ä. VII. 2; weitere Ä. mod. ($P^{(k)}$) VIII. 5.
Äquivalenzbereich I. 12.
echter Ä. I. 12; kleinster einem holoiden Bereiche [A] entstammender Ä. I. 12.
Äquivalenzmodul IX. 17.
Affinität III. 18.
Algebra I. 1, IV. 8, VII. 1.
Fundamentalsatz der A. IV. 27, 28
Algebraische.
A. Divisoren IX. 8; a. Funktion IV. 7; a. Größe I. 1, IV. 7; a. Mannigfaltigkeit V. 6; a. Methode IV. 8; a. Theorie der linearen diophantischen Systeme VII. 8. 9; a. Zahl I. 1, III. 21, IV. 7; absolut a. Größe IV. 7; absolut a. Größe mod. ($P^{(k)}$) VIII. 9; (einem Gattungsbereiche entstammende) ganze a. Form IX 2, 3; ganze a. Größe eines Gattungsbereichs IX, 2; in Bezug auf einen orthoiden Bereich (A) a. Größe IV. 7, IX. 1.
Allgemeine.
A. Form IV. 1, VI. 1; a. Gleichung n^{ten} Grades IV. 26; a. Gleichung zweiten Grades V. 6; a. (homogene) lineare Transformation II. 19.
Allgemeines Formensystem VI. 1.
Analysis I. 1, IV. 7.
Grenzwerte der A. IV. 21.
Analytische.
A. Funktionen VII. 8; a. Zahlentheorie IX. 13.
Arithmetik I. 1, IV. 8, VII. 1.

Arithmetische.
A. Auflösung der homogenen linearen diophantischen Gleichungen VIII. 10—18; a. Methode IV. 8; a. Theorie der algebraischen Größen IX. 1; a. Theorie der linearen diophantischen Systeme VII. 8.
Association IX. 8.
Associativ I. 2, 3.
Associierte Größen IX. 8.
Auflösung.
A. der linearen Kongruenz $AX \equiv B$ VIII. 1.

Baltzer V. 15.
Basis eines Rationalitätsbereichs IV. 22.
Bereich.
B. $[A, x]$ II. 1; B. $[A, x_1, \ldots, x_m]$ II. 2; B. $[\Gamma]_w$ der einem Gattungsbereiche entstammenden ganzen Formen IX. 3; B. $[\Gamma]$ der ganzen algebraischen Größen eines Gattungsbereichs IX. 3; B. der rationalen Zahlen I. 1, IV. 20; B. [1] I. 4; B. (1) I. 4; B. $[1], x_1, \ldots, x_k] \left(\mathrm{mod.}\,(P^{(k)})\right)$ VIII. 2; B. $[1], x_1, \ldots, x_k, x_{k+1}, \ldots, x_m]$ $\left(\mathrm{mod.}\,(P^{(k)})\right)$ VIII. 2; B. $([1], x_1, \ldots, x_k^l x_{k+1}, \ldots, x_m)$ $\left(\mathrm{mod.}\,(P^{(k)})\right)$ VIII. 2; B. $[\mathfrak{G}]$ IX. 7; B. $(\mathfrak{G})$ IX. 10; B. $\sqrt{-k}$ I. 7; B. $\sqrt{-5}$ I. 8, IX. 7; absoluter Rationalitätsb. IV. 20; Äquivalenzb. I. 12; Diophantischer B. VII. 1; Divisorenb. VII. 3; echter holoider B. I. 4; echter Kongruenzb. I. 10; Galoisscher B. IV. 13; Galoisscher B. mod. $(P^{(k)})$ VIII. 9; Gattungsb. (einem orthoiden Bereiche entstammender) IV. 14; Gattungsb. mod. $(P^{(k)})$ (einem pseudoorthoiden Bereiche entstammender) VIII. 9; holoider B. I. 4; hyperorthoider B. IV. 9; Infinitesimalb. erster Ordnung V. 8; kleinster einem holoiden Bereiche [A] entstammender Äquivalenzb. I. 12; kleinster orthoider B., der die Wurzel einer irreduziblen Gleichung enthält, IV. 7; kleinster pseudoorthoider B., der die Wurzel einer Kongruenz enthält, VIII. 9; Kongruenzb. I. 10; natürlicher Rationalitätsb. IV. 20; orthoider B. I. 4, IV. 9, 22; pseudoholoider B. VIII. 2; pseudoorthoider B. VIII. 2; Rationalitätsb. IV. 20; Stammb. (eines Gattungsbereichs) IV. 14; unechter holoider B. I. 4; vollständiger Gattungsb. IX. 10; vollständiger holoider B. I. 6; vollständiger pseudoholoider B. VIII. 2; wohldefinierter B. III. 1, IV. 3, 16; wohldefinierter vollständiger B. III. 8; zugeordneter orthoider B. I. 4, III. 12; zugeordneter pseudoorthoider B. VIII. 2.
Bestimmte Gleichungssysteme VI. 14, 15.
Brill VII. 13.
Bezoutsches Theorem VI. 16.

Charakteristik eines Wurzelsystems VII. 13—15.
Charakteristische Gruppe einer Gleichung IV. 24, 25.

Dedekind I. 2, 8, III. 4, 5, IV. 22, IX. 1, 8, 13, 27.
Dedekindscher Hilfssatz III. 4.
Derivation.
Grundgesetze der D. II. 5.
Derivierte.
Erste D. II. 5; höhere D. II. 5, 6.
Determinante.
D. der linearen Transformation II. 18; D. $\left|\mathfrak{f}_{rs}\right|$ II. 15; D. $\left|x_{i_1}^{j_1} x_{i_2}^{j_2} \ldots x_{i_\varrho}^{j_\varrho}\right|$ II. 12; D. $\left|x_{k+i}^{m-k-j}\right|$ II. 11; Funktionald. V. 14; Sylvestersche D. III. 14, VI. 4.
Determinanten-Matrix III. 4.
Differentialrechnung II. 5, V. 14.
Differenzenprodukt II. 11.
Dimension.
D. einer Form II. 2; D. einer Gleichung III. 19.
Diophantische Gleichung III. 19.
Diophantischer Bereich VII. 1.
Dirichlet I. 2.
Discriminante.
D. als symmetrische Form III. 25; D. der Gattung IX. 30; D. einer Form III. 22; D. einer Gleichung

IV. 13; D. einer Größe des Gattungsbereichs IX. 14; D. eines allgemeinen Formensystems VI. 21; D. eines Systems homogener Formen VI. 26; D. eines Systems von Formen, deren jede das Produkt allgemeiner linearer Formen ist, VI. 24; D. von n wirklichen Größen des Gattungsbereichs IX. 30; Fundamentaleigenschaften der D. einer Form III. 23; Grundeigenschaften der D. eines allgemeinen Formensystems VI. 23, 25, 26; Invarianteneigenschaft der D. VI. 27.
Discriminantenform der Gattung IX. 31.
Discriminantensystem, fundamentales IX. 30.
Distributiv I. 3.
Division I. 1, 4.
Divisionsverfahren, gewöhnliches III. 1.
Divisoren, algebraische IX. 8.
Divisorenbereich VII. 3.
Divisorenkette VII. 5.
Endliche D. VII. 5.
Divisorensystem VII. 2.
D. der Hauptklasse VII. 10; D., für welches ein vollständiges Restsystem existiert, VIII. 1; äquivalente D.-e VII. 2; komponiertes D. VII. 3; Komposition von D.-en VII. 3; mod. $(P^{(k)})$ äquivalente D.-e VIII. 5; Prim-D. VII. 4; Produkt von D.-en VII. 3; relativ prime D.-e VII. 2; relativ prime D.-e mod. $(P^{(k)})$ VIII. 5; Stufenzahl des D.-s VII. 10; unzerlegbares oder irreduzibles D. VII. 4.
Doppeltes Element einer Mannigfaltigkeit V. 6.

Echte irreduzible Größe I. 5.
Echter.
E. Äquivalenzbereich I. 12; e. holoider Bereich I. 4; e. Kongruenzbereich I. 10; e. Teiler I. 5, IX. 10; e. Teiler der Null IV. 8, 9.
Echtes Modulsystem I. 10, VII. 2.
Eigentlich primitive Form IX. 13.
Eingliedriges Modulsystem I. 11.
Einheit I. 5.
Absolute E. I. 3, IV. 6.
Einheiten.
E. des Äquivalenzbereichs I. 12; E. des Bereichs [$\mathfrak{G}$] IX. 7.
Einheitsform III. 9, IX. 4.
Eisenstein IV. 4.
Elementare symmetrische Form II. 11, VI. 18.
Elemente.
E. einer Mannigfaltigkeit III. 21, V. 6; E. eines Modulsystems I. 10; E. eines Rationalitätsbereichs IV. 21; doppelte E. einer Mannigfaltigkeit V. 6; mehrfache E. einer Mannigfaltigkeit V. 6; singuläre E. einer Mannigfaltigkeit V. 6; unendliche E. einer Mannigfaltigkeit V. 6.
Eliminante VI. 15.
Eliminationsmethode, Kroneckersche V. 2.
Eliminationsprinzip, Kroneckersches III. 18, V. 2.
Eliminationsproblem IV. 21.
Eliminationstheorie.
Fundamentalproblem der E. V. 1.
Endliche Divisorenkette VII. 5.
Engere.
E. Äquivalenz VII. 2; e. Äquivalenz mod. $(P^{(k)})$ VIII. 5.
Enthalten.
Begriff des E. VII. 2, 4; Begriff des E. mod. $(P^{(k)})$ VIII. 5.
Erhaltung der auf die Teilbarkeit bezüglichen Eigenschaften eines orthoiden Bereichs III. 13; IX. 7.
Euklidischer Algorithmus III. 11.
Euler III. 14.
E.sche Formeln II, 16; E.s Formelreihe für eine homogene Form II. 9.

Fläche V. 6.
F., welche eine Gerade vollständig enthält, V. 6.
Folge von Substitutionen IV. 23.
Form II. 2.
F. einer Unbestimmten, die einer F. von n Unbestimmten entspricht, II. 4; F. von α_u IX. 5; F. $P^{(k)}(z)$ II. 11; absolut ganze F. IX. 4; absolut irreduzible F. IV. 18; aequ. mod. P irreduzible F. IX. 17; aequ. mod. P Primf. IX. 18; allgemeine F. IV. 1, VI, 1; Discriminantenf.

der Gattung IX. 31; eigentliche primitive F. IX. 13; (einem Gattungsbereiche entstammende) ganze algebraische F. IX. 2, 3; Einheitsf. III. 9, IX. 4; elementare symmetrische F. II. 11, VI. 18; Fundamentalf. des Gattungsbereichs IX. 24; holoide F. III. 12; homogene F. II 8; irreduzible F. mod. (S) VIII. 1; kritische Primf. IX. 27; lineare F. IV. 3, 18; orthoide F. III. 12; Primf. IV. 2; Primf. im rationalen Formenbereiche IV. 3; Primf. im rationalen und ganzen Formenbereiche IV. 2; Primform in einem orthoiden Formenbereiche IV. 3; primitive F. III. 9, IX. 4; rationale und ganze Form des Bereichs $[1], x_1, \ldots, x_k, x_{k+1}]$ (mod. $(P^{(k)})$) VIII. 7; reduzierte F. II. 13; reguläre F. II. 19; reguläre F. in Bezug auf x_i II. 19; reguläre F. mod. $(P^{(k)})$ VIII. 4; relativ ganze F. IX. 4; Resolventen-F. III. 18; Resolventen-F. mod. $(P^{(k)})$ VIII. 6, 7; symmetrische F. II. 10, 14; symmetrische F. mehrerer Größensysteme VI. 18; transformierte F. II. 18; typische symmetrische F. VI. 18.

Formen.
Konjugierte F. IV. 16; voneinander abhängige F. V. 14; voneinander unabhängige F. V. 14.

Formensystem, allgemeines VI. 1.

Frobenius V. 15.

Fundamentaleigenschaften.
F. der Discriminante einer Form III. 23; F. der Resultante zweier Formen III. 15, 16; F. der Resultante eines allgemeinen Formensystems VI. 5.

Fundamentales Discriminantensystem IX. 30.

Fundamentalform des Gattungsbereichs IX. 24.

Fundamentalgleichung der Gattung IX. 24.

Fundamentalgröße des Gattungsbereichs IX. 24.

Fundamentalproblem.
F. der Eliminationstheorie V. 1; F.-e der vollständigen Auflösung eines Systems linearer diophantischer Gleichungen für einen diophantischen Bereich VII. 1.

Fundamentalsatz.
F. der Algebra IV. 27, 28; F. für die Theorie der Abbildung V. 10; F. für vollständigen Bereichen entstammende Formen III. 8; Gaußscher F. IV. 27; Kroneckerscher F. III. 5—7; Verallgemeinerung des Kroneckerschen F. VIII. 5.

Fundamentalsystem VIII. 2, IX. 1.
F. absolut ganzer Größen IX. 15; F. (absolut) ganzer algebraischer Zahlen IX. 16; F. der Gattung IX. 14; F. der in Bezug auf einen orthoiden Bereich relativ ganzen Größen IX. 15; F. idealer ganzer Größen IX. 24, 25; F. wirklicher ganzer Größen IX. 21—23.

Funktion.
Algebraische F. IV. 7; analytische F. VII. 8; ganze F. II. 2, 16, 17; rationale F. IV. 20; rationale F. der Wurzeln einer Gleichung IV. 15; transcendente F. IV. 21.

Funktionen, Theorie der algebraischen IX. 1,

Funktional, ganzes IX. 8.

Funktionaldeterminante V. 14.
Irreduzibilität der F. VI. 22.

Galois IV. 11, 21, 24.

Galoissche.
G. imaginäre Größen VIII. 9; G. Resolvente IV. 11, 13; G. Theorie der algebraischen Gleichungen IV. 26.

Galoisscher.
G. Bereich IV. 13; G. Bereich mod. $(P^{(k)})$ VIII. 9; G. Gattungsbereich IV. 14.

Galoissches Prinzip IV. 24.

Ganze.
G. algebraische Größe eines Gattungsbereichs IX. 2; g. Funktion II. 2, 16, 17; g. ideale Größe IX. 10; absolut g. Form IX. 4; absolut g. Größe IX. 4; (einem Gattungsbereiche entstammende) g. algebraische Form IX. 2, 3; in Bezug auf $[A, x_1, \ldots, x_m]$ rationale und g. Größe des Gattungs-

bereichs IX. 2; rationale und g. ideale Größe IX. 9; relativ g. Form IX. 4; relativ g. Größe IX. 4.
Ganzes Funktional IX. 8.
Gattung IV. 15.
G., unter einer G. enthalten, IV. 15; absolute Invariante der G. IX. 30; Discriminante der G. IX. 30; Discriminantenform der G. IX. 31; Fundamentalgleichung der G. IX. 24; Fundamentalsystem der G. IX. 14; Invariante der G. IX. 29; Singularitäten der G. IX. 31.
Gattungsbereich.
G., dessen Stammbereich selbst schon ein G. ist, IV. 16; (auf die additive und multiplikative Verknüpfung bezügliche) Eigenschaften eines G.-s IX. 1; konjugierte G.-e IV. 14; einem orthoiden Bereiche entstammender G. IV. 14; (einem pseudoorthoiden Bereiche entstammender) G. mod. $(P^{(k)})$ VIII. 9; Galoisscher G. IV. 14; vollständiger G. IX. 10; wirklicher G. IX. 10.
Gauß I. 4, 11, II. 3, III. 12, VIII. 2, IX. 1.
Gaußscher.
G. Satz für die Zerlegung rationaler und ganzer Formen III. 12; G. Fundamentalsatz IV. 27.
Gaußsches Prinzip II. 14.
Gebilde.
G. verschiedener Ausdehnung V. 6; absolut irreduzibles G. V. 7.
Gebrochene ideale Größe IX. 10.
Gemischte Mannigfaltigkeit $h+1$-ter Stufe V. 6.
Gemischtes System $h + 1^{\text{ter}}$ Stufe V. 6.
Gesamtheit.
G. der algebraischen Zahlen IV. 22; G. der komplexen Zahlen IV. 22; G. der reellen Zahlen IV. 22.
Gesamtresolvente V. 4.
Gewicht VI. 5.
Gewöhnliches.
G. Additionsgesetz I. 2; g. Divisionsverfahren III. 1; g. Gleichungssystem VI. 14, 15; g. Multiplikationsgesetz I. 3.
Gleichung.
G. $x^2 = 2$ IV. 7; allgemeine G. n^{ten} Grades IV. 26; allgemeine G. zweiten Grades V. 6; aus einem orthoiden Bereiche (A) entstammende G. n^{ten} Grades mit einer Unbekannten IV. 5; diophantische G. III. 19; Fundamentalg. der Gattung IX. 24; im orthoiden Bereiche (A) irreduzible G. IV. 5; in einem Bereiche lösbare G. I. 4; lineare G. V. 6; Lösung einer G. III. 19; Wurzel einer G. III. 19; IV. 6.
Gleichungen.
Problem der Theorie der G. III. 19; System homogener G. VI. 13; System linearer diophantischer G. VII. 1.
Gleichungssystem V. 1.
Bestimmtes G. VI. 14, 15; gemischtes G. $h + 1^{\text{ter}}$ Stufe V. 6; gewöhnliches G. VI. 14, 15; in einem orthoiden Bereiche irreduzibles G. V. 7; reines G. $h + 1^{\text{ter}}$ Stufe V. 6; singuläres G. VI. 30; transformiertes G. V. 2; unbestimmtes G. VI. 14, 15, 30.
Gleichungssystems.
Einfacher Fall des G. VII. 14; im Unendlichen liegende Lösungen eines G. VI. 13; Inhalt des G. V. 5; Lösung des G. III. 19, 20; Wurzelsystem des G. III. 19.
Gordan VII. 6.
Grad.
G. einer dem Bereiche {A} entstammenden $m - h - 1$-fachen Mannigfaltigkeit V. 6; G. einer Form II. 2; G. einer Gleichung III. 19; G. eines Primideals IX. 12.
Grenzwerte der Analysis IV. 21.
Größe.
Absolut algebraische G. IV. 7, IX. 1; absolut algebraische G. mod. $(P^{(k)})$ VIII. 9; absolut ganze G. IX. 4; adjungierte G. IV. 5; algebraische G. I. 1, IV. 7; associierte G. IX. 8; echte irreduzible G. I. 5; Fundamentalg. des Gattungsbereichs IX. 24; Galoissche imaginäre G. VIII. 9; ganze algebraische Gr. des Gattungsbereichs IX. 2, 3; ganze ideale G. IX. 10; gebrochene ideale G. IX. 10; holoide G. III. 12; ideale G. IX. 1; ideale G. des

Gattungsbereichs (Γ) IX. 10; ideale G. des Bereichs $[\Gamma]$ IX. 8; ideale G. im engeren Sinne des Wortes IX. 8; ideale G. im weiteren Sinne des Wortes IX. 8; in Bezug auf den orthoiden Bereich (A) algebraische Größe IV. 7, IX. 1; in Bezug auf $[A, x_1, \ldots, x_m]$ rationale G. eines Gattungsbereichs IX. 1; in Bezug auf $[A, x_1, \ldots, x_m]$ rationale und ganze G. eines Gattungsbereichs IX. 2; irreduzible G. I. 5, IX. 10; Maßg. IV. 7; mathematische G. I. 1; orthoide G. III. 12; Primg. I. 5, IX. 10; rationale und ganze ideale G. IX. 9; relativ ganze G. IX. 4; singuläre G. I. 3, IV. 9; transcendente G. IV. 21; transcendente Zahlengröße IV. 21; unbeschränkt veränderliche G. in $\{A\}$ V. 1; unendlich große G. IV. 9; unendlich kleine G. IV. 9; unendlich kleine G. erster Ordnung V. 8.

Größen, konjugierte IV. 14.

Größter gemeinschaftlicher.
G. g. Inhalt zweier Divisorensysteme VII. 2; g. g. Inhalt zweier Divisorensysteme mod. $(P^{(k)})$ VIII. 5; g. g. Teiler I. 6, IX. 7, 9; g. g. Teiler zweier Formen III. 11, 17; g. g. Teiler zweier Hauptideale IX. 13.

Gruppe.
G. von Permutationen IV. 23; G. von Substitutionen IV. 23; charakteristische G. einer Gleichung IV. 24, 25.

Hancock VII. 8.

Hauptdarstellung.
H. einer Mannigfaltigkeit m^{ter} Stufe V. 10; H. einer reinen algebraischen Raumkurve V. 9; H. einer reinen Mannigfaltigkeit V. 9, 10; H. einer reinen Mannigfaltigkeit erster Stufe V. 10.

Hauptideal IX. 13.

Hauptklasse, Divisorensystem der VII. 10.

Hauptlösung V. 8.

Hensel VII 8, IX. 24, 27, 28.

Hermite IV. 21.

Hesse III. 14.

Hilbert VII. 6, 16.

Hilberts Satz VII. 6, 16.

Holoide.
H. Form III. 12; h. Größe III. 12.

Holoider.
H. Bereich I. 4; echter h. Bereich I. 4; unechter h. Bereich I. 4; vollständiger h. Bereich I. 6.

Homogene.
H. Form II. 8; allgemeine h. lineare Transformation II. 19.

Höhe der Glieder einer Form II. 3.

Hurwitz III. 5.

Hyperorthoider Bereich IV. 9.

Ideal IX. 8.
Haupti. IX. 13.

Ideale.
I. Größe IX. 1; i. Größe des Gattungsbereichs (Γ) IX. 10; i. Größe des Bereichs $[\Gamma]$ IX. 8; i. Größe im engeren Sinne des Wortes IX. 8; i. Größe im weiteren Sinne des Wortes IX. 8; ganze i. Größe IX. 10; gebrochene i. Größe IX. 10; rationale und ganze i. Größe IX. 9.

Identische Substitution IV. 24.

Imaginäre Größe, Galoissche VIII. 9.

Imaginärer Punkt einer Geraden IX. 8.

Infinitesimalbereich erster Ordnung V. 8.

Inhalt.
I. des Gleichungssystems V. 5; größter gemeinschaftlicher I. zweier Divisorensysteme VII. 2; größter gemeinschaftlicher I. zweier Divisorensysteme mod. $(P^{(k)})$ VIII. 5.

Invariant III. 9, IX. 5.

Invariante.
I. der Gattung IX. 30; absolute I. der Gattung IX. 31.

Invarianteneigenschaft.
I. der Discriminante VI. 27; I. der Resultante VI. 12.

Inverse Substitution IV. 24.

Irrationalität, reelle quadratische IV. 5.

Irreduzibilität der Funktionaldeterminante VI. 22.

Irreduzibilitätssätze V. 7.

Irreduzible.
I. Form mod. (S) VIII. 1; i. Größe I. 5, IX. 10; absolut i. Form IV. 18; absolut i. Mannigfaltigkeit V. 7; aequ. mod. P. i. Form IX. 17; echte i. Größe I. 5; im orthoiden Bereiche (A) i. Gleichung IV. 5; in Bezug auf einen orthoiden Bereich i. Teilresolvente $h + 1^{ter}$ Stufe V. 7; in einem orthoiden Bereiche i. Mannigfaltigkeit V. 7.
Irreduzibles.
I. Divisorensystem VII. 4; im orthoiden Bereiche (A) i. Gleichungssystem V. 7; absolut i. Gebilde V. 7.
Irreguläre Primzahl eines Gattungsbereichs IX. 25.
Isobarisch VI. 5.

Jacobi V. 14.
Junker VI. 18.

Kegelschnitt, nicht zerfallender V. 6.
Klassenanzahl der idealen Größen IX. 13.
Klasseneinteilung der idealen Größen IX. 13.
Klein IV. 26.
Kleinster.
K. einem Bereiche [A] entstammender Äquivalenzbereich I. 12; k. orthoider Bereich, der die Wurzel einer irreduziblen Gleichung enthält, IV. 7; k. pseudoorthoider Bereich, der die Wurzel einer Kongruenz enthält, VIII. 9.
Koeffizient I. 1, 2.
Koeffizienten der Transformation II. 18.
Kollineation VI. 13.
Kombination IV. 27.
Kommutativ I. 2, 3.
Kommutatives Prinzip VII. 3.
Komplementärer Teiler III. 1.
Komplexe Zahlen III. 21, IV. 5, 6.
Komponiertes Divisorensystem VII. 3.
Komposition von Divisorensystemen VII. 3.
Kompositionsfaktoren VII. 3.
Kongruente Größen in Bezug auf ein Modulsystem I. 10.
Kongruenz.
K. n^{ten} Grades mit einer Unbekannten VIII. 4; allgemeine lineare K. VIII. 16; Auflösung der linearen K. $AX \equiv B$ VIII. 1; Lösungen einer linearen K. VII. 6; Wurzel einer K. VIII. 4, 9.
Kongruenzbereich I. 10.
Echter K. I. 10.
Konjugierte.
K. Formen IV. 16; k. Gattungsbereiche IV. 14; k. Größen IV. 14; k. Lösungen V. 8; k. Wurzeln IV. 14.
Koordinaten V. 6.
Koordinatentransformation V. 3.
Körper IV. 22.
Kritische Primform IX. 27.
Kronecker I. 1, 4, 11, II. 2, 4, 13, III. 5, 18, 23, IV. 1, 14, 16, 20, 21, 24, V. 2, 10, 11, VI. 1, 25, 26, VII. 2, 4, IX. 1, 4, 5, 8, 13, 15, 24, 25, 27, 28, 29.
Kroneckers Relationen II. 16.
Kroneckersche Eliminationsmethode V. 2.
Kroneckersches Eliminationsprinzip III. 18, V. 2.
Kroneckerscher Fundamentalsatz III. 5—7; Verallgemeinerung desselben VIII. 5.
Kummer IX. 1, 8.
Kummersche Äquivalenz IX. 13.

Lagrangesche Interpolationsformel II. 17, IV. 1.
Lindemann IV. 21.
Lineare.
L. Form IV. 3, 18; l. Gleichung V. 6; l. Mannigfaltigkeit V. 12; l. Substitution II. 18; l. Transformation II. 18; allgemeine homogene l. Transformation II. 19; allgemeine l. Kongruenz VIII. 16; reziproke l. Transformation II. 18.
Linie V. 6.
Lösbarkeit.
L. der Kongruenz $\sum_{j=1}^{h} f_j X_j \equiv 1 \pmod{(P^{(k)})}$ VIII. 6; L. einer li-

nearen diophantischen Gleichung VIII. 8.
Lösung.
L. einer dem orthoiden Bereich (A) entstammenden Gleichung n^{ten} Grades mit einer Unbekannten im Bereich (A) IV. 5; L. einer Gleichung III. 19; L. eines Gleichungssystems III. 19, 20; Bestimmung einer L. einer linearen diophantischen Gleichung VIII. 8. Hauptl. V. 8; im Unendlichen liegende L. eines Gleichungssystems VI. 13; Multiplizität der L. V. 5, VI. 30; wirkliche L. eines Systems homogener Gleichungen VI. 13.
Lösungen.
L. einer homogenen linearen Kongruenz VII. 6; konjugierte L. V. 8.

Mannigfaltigkeit.
Absolut irreduzible M. V. 7; algebraische M. V. 6; dem holoiden Bereiche [A] entstammende $m-k$-fache M. III. 21; dem Bereiche {A} entstammende $m-h-1$-fache M. V. 6; Element der M. III, 21, V. 6; gemischte M. $h+1^{ter}$ Stufe V. 6; Hauptdarstellung einer M. m^{ter} Stufe V. 10; Hauptdarstellung einer reinen M. V. 9, 10; Hauptdarstellung einer reinen M. erster Stufe V. 10; in einem orthoiden Bereiche irreduzible M. V. 7; lineare M. V. 12; mehrfaches (doppeltes) Element einer M. V. 6; reine M. $h+1^{ter}$ Stufe V. 6; singuläres Element der M. V. 6; transcendente M. V. 6; unendliche Elemente einer M. V. 6.
Maßgröße IV. 7.
Mathematische Größe I. 1.
Matrix (Determinanten-) III. 4.
Mehrfache Wurzel einer Gleichung IV. 13.
Mehrfacher Teiler einer Form III. 22.
Mehrfaches Element einer Mannigfaltigkeit V. 6.
Mertens VI. 4, 5, 9.
Methode.
Algebraische M. IV. 8; arithmetische M. IV. 8.
Minimalresolvente V. 11.
Modulsystem I. 10.
Echtes M. I. 10, VII. 2; eingliedriges M. I. 11; h-gliedriges M. I. 10, VII. 2; Prim-M. VII. 4.
Modulsysteme, äquivalente VII. 2.
Modulsystems, Elemente des I. 10.
Modulus I. 11.
Molk III. 5, IV. 16, V. 5, 10.
Multiplikation I. 1.
Multiplikationsgesetz, gewöhnliches I. 3.
Multiplizität.
M. der Lösung V. 5, VI. 28—30; M. des Wurzelsystems VI. 15.

Natürliche Primzahl I. 5.
Natürlicher Rationalitätsbereich IV. 20.
Netto V. 5.
Newton-Girardsche Formeln IX. 28.
Noether VII. 13, 14.
Noetherscher Satz VII. 8.
Verallgemeinerter N. VII. 13.
Norm IX. 1.
Null I. 2, 3, IV. 6, VIII. 2.
Echter Teiler der N. IV. 8, 9; Teiler der N. IV. 9.
Nullstelle III. 19.

Ordnung.
O. einer Gattung IV. 15; O. einer Gleichung IV. 12; O. einer Größe des Gattungsbereichs IV. 15; O. einer Gruppe IV. 24; O. eines Gattungsbereichs IV. 15; O. eines Rationalitätsbereichs IV. 22.
Orthoide.
O. Form III. 12; o. Größe III. 12.
Orthoider.
O. Bereich I. 4, IV. 9, 22; kleinster o. Bereich, der die Wurzel einer Gleichung enthält, IV. 7; zugeordneter o. Bereich I. 4, III. 12.

Permutation II. 14, IV. 10, 14, 23.
Permutationen, Gruppe von P. IV. 23.
Poisson VI. 17.
Poissonsche Darstellung der Resultante VI. 17.
Polynomischer Lehrsatz II. 7.
Primdivisorensystem VII. 4.

Primform IV. 2.
P. im rationalen Formenbereiche IV. 3; P. im rationalen und ganzen Formenbereiche IV. 2; P. in einem orthoiden Formenbereiche IV. 3; P. aequ. mod. P IX. 18; kritische P. IX. 27.
Primgröße I. 5, IX. 10.
Primideale IX. 12.
Verbundene P. IX. 12.
Primitive.
P. Form III. 9, IX. 4; eigentlich p. Form IX. 13.
Primmodulsystem VII. 4.
Primsystem VII. 4.
Absolutes P. VII. 4; absolutes P. in $[1], x_1, \ldots, x_k]$ VIII. 1—4, 8.
Primteiler IV. 2.
Primzahl (natürliche) I. 5; irreguläre P. eines Gattungsbereichs IX. 25.
Prinzip.
Galoissches P. IV. 24; Gaußsches P. II. 14; kommutatives P. VII. 3; Kroneckersches Eliminationsp. III. 18, V. 2.
Produkt I. 3, II. 1, IV. 6.
P. von Divisorensystemen VII. 3; P. von Substitutionen IV. 23.
Produktsatz der Resultantentheorie VI. 11.
Pseudoholoider.
P. Bereich VIII. 2; vollständiger p. Bereich VIII. 2.
Pseudoorthoider.
P. Bereich VIII. 2; kleinster p. Bereich, der die Wurzel einer Kongruenz enthält, VIII. 9; zugeordneter p. Bereich VIII. 2.
P-Systeme $k+1^{\text{ter}}$ Stufe VIII. 2.
Punkt V. 6.
Imaginärer P. einer Geraden IX. 8

Quadratische.
Reelle q. Irrationalität IV. 5.
Quotient III. 1.

Rados II. 12.
Rang.
R. einer Determinante V. 15; R. einer durch ein Gleichungssystem definierten Mannigfaltigkeit V. 6; R. einer Matrix V. 15; R. eines Gleichungssystems V. 6; R. eines orthoiden Formensystems V. 6.
Rationale.
R. Funktion IV. 20; r. Funktion der Wurzeln einer Gleichung IV. 15; r. Operationen V. 1; r. und ganze Form des Bereichs $[[1], x_1, \ldots, x_k, x_{k+1}] (\text{mod.}(P^{(k)}))$ VIII. 7; r. und ganze ideale Größe IX. 9; in Bezug auf $[A, x_1, \ldots, x_m]$ r. Größe eines Gattungsbereichs IX. 1; in Bezug auf $[A, x_1, \ldots, x_m]$ r. und ganze Größe eines Gattungsbereichs IX. 2; r. Wurzel einer Gleichung III. 12.
Rationalitätsbereich IV. 20.
Absoluter R. IV. 20; natürlicher R. IV. 20; Basis eines R.s IV, 22; Elemente eines R.s IV. 21.
Raum von m Dimensionen V. 6.
Raumkurve, Hauptdarstellung einer reinen algebraischen V. 9.
Reduktion der Auflösung der homogenen linearen diophantischen Gleichung VIII. 10—18.
Reduzierte.
R. Form II. 13; r. Resolvente V. 5.
Reelle quadratische Irrationalität IV. 5.
Reguläre.
R. Form II. 19; r. Form in Bezug auf x_i II. 19; r. Form mod. $(P^{(k)})$ VIII. 4.
Reich.
R. der algebraischen Funktionen von n Unbestimmten IV. 19; R. der algebraischen Zahlen IV. 19; R. der in Bezug auf einen orthoiden Bereich algebraischen Größen V. 1.
Reine Mannigfaltigkeit $h+1^{\text{ter}}$ Stufe V. 6.
Reines System $h+1^{\text{ter}}$ Stufe V. 6.
Relativ.
R. äquivalent I. 5, 12, IX. 13; r. ganze Form IX. 4; r. ganze Größe IX. 4; r. prime Divisorensysteme VII. 2; r. prime Divisorensysteme mod. $(P^{(k)})$ VIII. 5.
Relative Äquivalenz I. 5, IX. 13.
Resolvente.
Galoissche R. IV. 11, 13; Gesamtr. V. 4; in Bezug auf einen orthoiden Bereich irreduzible Teilr. $h+1^{\text{ter}}$

Stufe V. 7; Minimalr. V. 11; reduzierte R. V. 5; Teilr. V. 4; vollständige Teilr. $h+1^{ter}$ Stufe V. 4.
Resolventenform III. 18.
R. mod. $(P^{(k)})$ VIII. 6, 7.
Rest III. 1.
Restsystem, vollständiges VII. 8, VIII. 1.
Resultante.
R. allgemeiner linearer Formen VI. 11; R. als symmetrische Form III. 24; R. eines allgemeinen Formensystems VI. 3; R. eines Systems homogener Formen VI. 12; R. spezieller Formen VI. 3; R. zweier Formen III. 15; Bildungsgesetz der R. VI. 10; Fundamentaleigenschaften der R. zweier Formen III. 15, 16; Grundeigenschaften der R. eines allgemeinen Formensystems VI. 5; Invarianteneigenschaft der R. VI. 12; Poissonsche Darstellung der R. VI. 17.
Reziproke lineare Transformation II. 18.
Richelot III. 14.
Runge IV. 1.

Schar V. 13.
k-gliedrige Sch. V. 13.
Schläfli VI. 18.
Schönemann VIII. 2.
Singularitäten der Gattung IX.
Singuläre. [31.
S. Fälle der Auflösung der homogenen linearen diophantischen Gleichung VIII. 14, 16, 17, 19; s. Größe I. 3, IV. 9.
Singuläres.
S. Element einer Mannigfaltigkeit V. 6; s. Gleichungssystem VI. 30.
Species, die vier I. 1.
Stammbereich (eines Gattungsbereichs) IV. 14.
Stufe.
St. der vollständigen Teilresolvente V. 4; St. einer durch ein Gleichungssystem definierten Mannigfaltigkeit V. 6; St. eines Gleichungssystems V. 6; St. eines orthoiden Formensystems V. 6.
Stufenzahl eines Divisorensystems VII. 10.
Substitution II. 10, IV. 23.
Identische S. IV. 24; inverse S. IV. 24; lineare S. II. 18.
Substitutionen.
Folge von S. IV. 23; Gruppe von S. IV. 23; Produkt von S. IV. 23.
Subtraktion I. 1, 2.
Summe I. 2, II. 1, IV. 6.
Sylvester III. 14.
Sylvestersche Determinante III. 14, VI. 4.
Symmetrische.
S. Form II, 10, 14; s. Form von mehreren Größensystemen VI. 18; elementare s. Form II. 11, VI. 18; typische s. Form VI. 18.
System.
S. homogener Gleichungen VI. 13; S. linearer diophantischer Gleichungen VII. 1; absolutes Prims. in $[1], x_1, \ldots, x_k]$ VIII. 1—8; fundamentales Discriminantens. IX. 30; Fundamentals. VIII. 2, IX. 1; Fundamentals. absolut ganzer Größen IX. 15; Fundamentals. der (absolut) ganzen algebraischen Zahlen IX. 16; Fundamentals. der Gattung IX. 14; Fundamentals. der in Bezug auf einen orthoiden Bereich relativ ganzen Größen IX. 15; Fundamentals. idealer ganzer Größen IX. 24, 25; Fundamentals. wirklicher ganzer Größen IX. 21—23; gemischtes S. $h+1^{ter}$ Stufe V. 6; P.-S. $k+1^{ter}$ Stufe VIII. 2; Prims. VII. 4; reines S. $h+1^{ter}$ Stufe V. 6; vollständiges Rests. VII. 8, VIII. 1.

Teilbarkeit.
T. der Formen III. 2; T. mod. (S) VIII. 1; T. nach einem Äquivalenzmodulus IX. 17; auf die T. bezügliche Eigenschaften der idealen Größen IX. 10; Elementargesetze der T. I. 5. Erhaltung der auf die T. bezüglichen Eigenschaften eines orthoiden Bereichs III. 13, IX. 7; Theorie der T. im Bereiche $[1], x_1, \ldots, x_m]$ $(\mathrm{mod}.P^{(k)})$ VIII. 2.
Teilbarkeitsbegriffs, Erweiterung des VII. 2.

Teilbarkeitsgesetze.
T. im Bereiche [1] IV. 1; T. im Bereiche $[[1], x_1, \ldots, x_m]$ der rationalen und ganzen Formen IV. 1, II. 10, IV. 23.
Teiler I. 5.
T. der Null IV. 9; T. einer rationalen und ganzen Form IV. 1; Teiler einer rationalen und ganzen Zahl IV. 1; echter T. I. 5, IX. 10; echter T. der Null IV. 8, 9; größter gemeinschaftlicher T. I. 6, IX. 7, 9; größter gemeinschaftlicher T. zweier Formen III. 11, 17; größter gemeinschaftlicher T. zweier Hauptideale IX. 13; komplementärer T. III. 1; mehrfacher T. einer Form III. 22; Primt. IV. 2.
Teilresolvente.
In Bezug auf einen orthoiden Bereich irreduzible T. $h+1^{ter}$ Stufe V. 7; vollständige T. $h+1^{ter}$ Stufe V. 4.
Theorie.
T. der algebraischen Funktionen einer Veränderlichen IX. 1; T. der Gleichungen III. 19; T. der Gleichungssysteme III. 19; algebraische T. der linearen diophantischen Systeme VII. 8, 9; arithmetische T. der algebraischen Größen IX. 1; arithmetische T. der linearen diophantischen Systeme VII. 8; Galoissche T. der algebraischen Gleichungen IV. 26.
Transcendente.
T. Funktion IV. 21; t. Größe IV. 21; t. Mannigfaltigkeit V. 6; t. Zahlengröße IV. 21.
Transformation.
Allgemeine (homogene) lineare T. II. 19; Determinante der linearen T. II. 18; Koeffizienten der T. II. 18; Koordinaten-T. V. 3; lineare T. II. 18; reziproke lineare T. II. 18.
Transformierte Form II. 18.
Transformiertes Gleichungssystem V. 2.
Type VI. 18.
Einförmige T. VI. 19; k-förmige T. VI. 19.
Typische symmetrische Form VI. 18.

Unabhängige.
Voneinander u. Formen V. 14; voneinander u. Wurzelsysteme V. 13.
Unbekannte III. 19.
Unbeschränkt veränderliche Größe in $\{A\}$ V. 1.
Unbestimmte II. 1, 2, V. 1.
U. Gleichungssysteme VI. 14, 15, 30; u. Zahl I. 1.
Unechter holoider Bereich I. 4.
Unendlich.
U. große Größen IV. 9; u. kleine Größen IV. 9; u. kleine Größe erster Ordnung V. 8.
Unendliche Elemente einer Mannigfaltigkeit V. 6.
Unendlichen.
Im U. liegende Lösung eines Gleichungssystems VI. 13.
Unzerlegbares Divisorensystem VII. 4.

Vahlen V. 11.
Variation II. 12.
Varietät V. 6.
Verallgemeinerter Noetherscher Satz VII. 13.
Verallgemeinerung des Kroneckerschen Fundamentalsatzes VIII. 5.
Verbundene Primideale IX. 12.
Verknüpfung I. 1.
Vielfaches I. 5.
Vollständige Teilresolvente $h+1^{ter}$ Stufe V. 4.
Vollständiger.
V. Gattungsbereich IX. 10; v. holoider Bereich I. 6; v. pseudoholoider B. VIII. 2; wohldefinierter v. Bereich III. 8.
Vollständiges Restsystem VII. 8, VIII. 1.

Waring VI. 18.
Weber IX. 1, 8.
Weierstraß IV. 8.
Weitere.
W. Äquivalenz VII. 2; w. Äquivalenz mod. $(P^{(k)})$ VIII. 5.
Wirkliche Lösung eines Systems homogener Gleichungen VI. 13.

Wirklicher Gattungsbereich IX.
Wohldefinierter. [10.
W. Bereich III. 1, IV. 3, 16; w. vollständiger Bereich III. 8.
Wurzel.
W. einer Kongruenz VIII. 4, 9; W. einer Gleichung III. 19, IV. 6; mehrfache W. einer Gleichung IV. 13; rationale W. einer Gleichung III. 12.
Wurzeln, konjugierte IV. 14
Wurzelsystem eines Gleichungssystems III. 19.
Wurzelsysteme, voneinander unabhängige V. 13.
Wurzelsystems.
Multiplizität des W. VI. 15; Charakteristik des W. VII. 13—15.

Zahl I. 1.
Z. e IV. 21; Z. π IV. 21; algebraische Z. I. 1, III. 21, IV. 7; komplexe Z. III. 21. IV. 5, 6; Primz. (natürliche) I. 5; Primz. (irreguläre) IX. 25; transcendente Z. IV. 21; unbestimmte Z. I. 1.
Zahlentheorie, analytische IX. 13.
Zerlegung.
Z. ganzer Größen in Primideale IX. 11, 21, 26—28; Z. einer irregulären Primzahl IX. 28; Z. einer orthoiden Form in Primformen IV. 3; Z. einer rationalen Form in Primformen IV. 3; Z. einer rationalen und ganzen Form in Primformen IV. 2; Z. einer rationalen und ganzen Zahl in Primfaktoren IV. 1.
Zufälligkeit III. 18, V. 2, 3.
Zugeordneter.
Z. orthoider Bereich I. 4, III. 12. z. pseudoorthoider Bereich VIII. 2.

PLEASE DO NOT REMOVE
CARDS OR SLIPS FROM THIS POCKET

UNIVERSITY OF TORONTO LIBRARY

P&A Sci.